Proceedings of the meeting of specialists on the reliability of mechanical components and systems for nuclear reactor safety

Research Establishment Risø, Roskilde

Publication date:
1970

Document Version
Publisher's PDF, also known as Version of record

Risø Report No. 214

Danish Atomic Energy Commission

Research Establishment Risø

Proceedings of the Meeting of Specialists on the Reliability of Mechanical Components and Systems for Nuclear Reactor Safety

Organized under the auspices of the Committee on Reactor Safety Technology (ENEA) with the co-operation of the Health and Safety Branch of the UKAEA and the European Communities (General Directorate of Industrial Affairs, and CCR, Ispra).
Hosted by the Danish Atomic Energy Commission at the Research Establishment Risø on 24-26 September 1969.

February, 1970

Sales distributors: Jul. Gjellerup, 87, Sölvgade, DK-1307 Copenhagen K, Denmark
Available on exchange from: Library, Danish Atomic Energy Commission, Risø, DK-4000 Roskilde, Denmark

U. D. C.
621.039.58

February, 1970 Risö Report No. 214

Proceedings of the Meeting of Specialists on the Reliability of Mechanical Components and Systems for Nuclear Reactor Safety

Organized under the auspices of the Committee on Reactor Safety Technology (ENEA) with the co-operation of the Health and Safety Branch of the UKAEA and the European Communities (General Directorate of Industrial Affairs, and CCR, Ispra). Hosted by the Danish Atomic Energy Commission at the Research Establishment Risö on 24 - 26 September 1969.

Abstract

Twenty-eight papers are presented from the four sessions of the meeting, dealing with the following subject fields: light mechanical systems and equipment; heavy dynamic mechanical systems and equipment; structures; relevant experience from various fields.

ISBN 07 550 0020 7

CONTENTS

Heavy Dynamic Mechanical Systems and Equipment

The Reliability of Emergency Core-Cooling Systems of Light-Water Nuclear Power Plants

W. Bastl, H. Gieseler
IMR
Munich
Germany

H. Maurer
Commission of the European Communities
Brussels
Belgium

Ontario Hydro Nuclear Generating Station - Safety and Production Reliability

R. J. Kelly
Ontario Hydro
Canada

Frequency and Causes of Failure to Components of Large Steam Turbines

M. Huppmann
Allianz Versicherungs-AG
Munich
Germany

Fiabilité Opérationelle d'une Machine - Fiabilité Prévisionnelle d'un Système Compremant N Machines en Parallele

P. Micheau
Société Bertin
Plaisir
France

A. Benmergui
EDF
Paris
France

Auslegung und Anordnung einer Reaktor-Beschickungsanlage auf Grund von Zuverlässigkeitsbetrachtungen

U. Hennings
Brown Boveri/Krupp
Reaktorbau GmbH
Mannheim
Germany

Demonstration of the Performance and Reliability of the G. E. Co. BWR Main Steamline Isolation Valves

I. M. Jacobs
General Electric Co.
San Jose, California
USA

Structures

Fracture Mechanics Approach to the Assessment of Reliability of Reactor Pressure Tubes

D. Basile, G. Volta
CCR,Euratom
Ispra
Italy

A Review of the Safety Aspects of the Design of Prestressed Concrete Pressure Vessels with Reference to Limit State Design

C. W. Yu, S. Gill
Imperial College of Science and Technology
London
U. K.

Analysis of a German Pressure Vessel and Boiler Drum Statistics

G. Mieze
IRS
Cologne
Germany

A Survey of Pressure Vessels Built to a High Standard of Construction

C. A. G. Phillips
AHSB
UKAEA
U. K.

R. G. Warwick
Associated Offices, Technical Committee
National and Vulcan Engineering Insurance Group
Manchester, U. K.

Relevant Experience from Various Fields

La Fiabilité des Propulseurs à Réaction Directe

A. Mihail
Bureau Véritas
Paris
France

Collecte et Utilisation des Informations Concernant le Comportement des Matériels

Mme G. Arnaud
Société Nationale pour l'Etude et la Construction des Moteurs d'Aviation
Paris
France

A Description of the Air Canada Unit Quality Record A. I. R. System II

K. E. Chapman
Air Canada
Maintenance Division

A Review and Discussion of Methods and Techniques of Acquiring, Disseminating, Exchanging and Utilizing Test Data and Failure Rate Data on Parts/Components on a Nation-wide Basis

S. Pollock
Naval Fleet Missile Systems
Corona, California
USA

Availability and Fault Analysis of Thermal Generating Equipment

J. E. Knudsen
NESA
Hellerup
Denmark

Reliability Aspects of Safety Evaluation of Nuclear Power Plants

S. Hattori
Chubu Electric Power Co.
Japan

K. Takemura
Tokyo University of Mercantile Marine
Japan

Aspects of Design Reliability of Pressure Tubes for Heavy Water Moderated Reactors

M. Montagnani, J. Putzeys
CCR, Euratom
Ispra
Italy

Reliability Considerations for Mechanical Components of Control Rod Drive Systems of Gas-cooled Power Reactors Operated in the European Community

J. Ehrentreich, H. Maurer
Commission of the European Communities
Brussels
Belgium

Quelques Modèles Markoviens de Fiabilité

M. Chatelain
EDF
Clamart
France

General Principles of a Safety Assessment Through Reliability Analysis of the Essor Plant

A. Cuoco, R. Galvagni
CNEN
Italy

F. Leonelli
Euratom, Ispra
Italy

Quelques Remarques sur la Fiabilité en Mécanique

C. Michel
Société Bertin
Plaisir
France

INTRODUCTION

This meeting was the third in a series of specialist discussions on the reliability of components and systems for nuclear reactor safety covering electronic, electromechanical and the latest mechanical equipment.

The meeting was organized by the Committee on Reactor Safety Technology (CREST) within the European Nuclear Energy Agency in co-operation with the Health and Safety Branch of the UKAEA and the European Communities (General Directorate of Industrial Affairs, and CCR, Ispra).

To facilitate reproduction and speed up publication, the papers are reproduced directly from the best available copies. Hardly any editorial alterations have been made, and the original pagination of the individual papers has been retained.

Thanks are extended to the staff of the Library of Risö for the preparation of the Proceedings.

P. Timmermann

AHSB (S) R 178

United Kingdom Atomic Energy Authority

THE RELIABILITY PREDICTION OF MECHANICAL INSTRUMENTATION EQUIPMENT FOR PROCESS CONTROL

G. Hensley
Control and Instrumentation Section,
Safeguards Division

1969
AUTHORITY HEALTH AND SAFETY BRANCH
Risley, Warrington, Lancashire

SUMMARY

Mechanical instrumentation equipment is often used in control and safety shutdown systems for such installations as nuclear reactors and chemical plants. The reliability of these systems is dependent, among other things, on the failure rates of the individual equipments which can be calculated by means of a prediction technique. By considering the effects of each component failure, and allocating the relevant failure rate for the component fault mode considered, a prediction can be made of the failure rate of a complete equipment of components. As an example, the effects of failure of some of the more important components of a simple pressure switch are analysed.

Typical failure rates are given for components and equipments, and the effects of common faults on achievable system reliability are discussed.

U.D.C. Nos:
62.004.6
621-5

Subject Category:
10

CONTENTS

INTRODUCTION

1. Mechanical equipment - consisting of mechanical, pneumatic and hydraulic components - is often used in control and safety shutdown systems for such installations as nuclear reactors and chemical plants. Where the overall reliability of a system of equipments of this type needs to be found, it is necessary to have a knowledge of the equipment failure rates as well as other factors such as the grouping of the equipments and the proof test interval. Equipment failure rates can be found as a result of sample testing, from field experience or by prediction. Where equipment of a new design is used and only few of the equipments have been manufactured prior to their installation in the plant, it is improbable that the failure rate will be known by means of sample testing or field experience. The prediction technique then becomes a useful way of assessing equipment failure rates.

PREDICTION TECHNIQUE

2. The prediction technique makes use of the fact that whilst an equipment may be new or untried, the majority of its components will not. Much information is now available relating to the failure rates of mechanical and pneumatic components[1,2] and examples of these, as applicable to the automatic protective systems of land-based nuclear installations, are given in Table 1. By considering the effects of each component failure and allocating the relevant failure rate for the component fault mode considered, the assessor can summate the individual failure rates for the different fault categories to find, for example, the "dangerous", "safe" and "overall" fault rates of the equipment. This technique can be illustrated by referring to Figure 1 which is a diagrammatic arrangement of a conventional type of pressure switch. Only a few of the more important components of the pressure switch are shown for clarity, the principle of operation being as described in the following text.

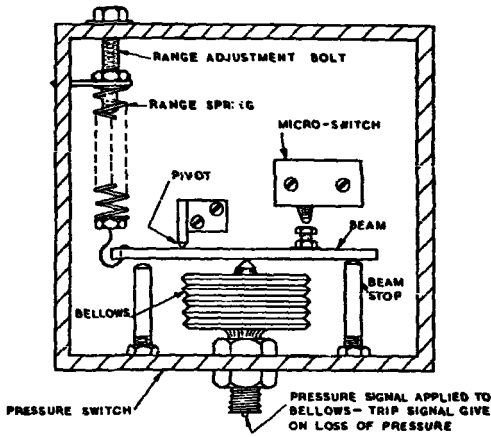
TABLE 1

Component Failure Rates

Type of component	Failure rate (faults/10^6 hours)
Bellows	5·0
Diaphragms, rubber	8·0
Gaskets	0·5
Springs, heavily stressed	1·0
lightly stressed	0·2
Pivots	1·0
Screws	0·5
Nuts, bolts, bars, etc.	0·02

3. When a pressure signal is applied to the bellows this expands, the free end of the bellows moving upwards causing the beam to move in an anticlockwise direction about the pivot. As the signal pressure increases, a point is reached where the micro-switch is actuated by the beam, this being the trip setting point. Acting against the force of the bellows is a spring, the tension of which (and hence the range of the switch) can be adjusted by means of the range adjustment bolt. For this application, it may be considered that a trip signal (a signal which restores plant safety by causing the shutdown system to trip and shut down the plant) is given when the pressure signal falls, i.e. a fail-safe fault on the loss of pneumatic supply.

4. Given the above information, the effects of failure of some of the switch components can be assessed. As can be seen from Figure 1, fracture of the spring would mean that there was no force opposing the action of the bellows so that the micro-switch would only be de-actuated when the bellows pressure fell to a very low level, perhaps a few percent of full scale deflection, instead of at the trip setting of, say, 50% f.s.d. This is obviously a fail-danger fault since a trip signal (micro-switch de-actuated) would only take place when the pressure signal had fallen to a level very much lower than that at which a trip signal should have been given. On the other hand, rupture of the bellows is a safe fault since this causes



COMPONENT	FAULT	CATEGORY	FAILURE RATE-FAULTS/10^6 HOURS	
			DANGEROUS	SAFE
SPRING	FRACTURE	DANGER	0·2	
BELLOWS	RUPTURE	SAFE		5·0
SCREWS-PIVOT(2)	LOOSEN	DANGER	1·0	
MICRO-SWITCH	RANDOM	25%d, 75%s	0·5	1·5
TOTAL = 5			1·7	6·5
ACTUAL TOTAL =30			2·9	11·7

FIG. 1. PRESSURE SWITCH FAILURE RATES.

a trip signal to be given immediately. A study of the effects of each fault enables a "fault category" column to be completed as in Figure 1, the failure rates for the components being added from Table I.

5. It can be seen that by summating the failure rates of the components which result in dangerous, and similarly safe failures, the fail-dangerous and fail-safe rates resulting from the failure of some half dozen components can be found (1·7 and 6·5 faults/10^6 hours, respectively). By adding together these two summated values, the total failure rate can be found for the number of components considered. A complete pressure switch could incorporate about thirty components, the overall failure rate for a particular switch having been predicted as 15 faults/10^6 hours or 0·13 faults/year.

6. A typical pneumatic transmitter could consist of some eighty components ranging from nuts and bolts having very low failure rates (0·02 faults/10^6 hours) to bellows, flapper-nozzle

or diaphragms which, in comparison, have high failure rates (5, 6 and 8 faults/10^6 hours, respectively). Normally there are about four or five of these "vulnerable" components in a transmitter but because of their comparatively high failure rates, this small percentage of the total number of components (say 5%) makes up some 50% of the total equipment failure rate. It follows then that if by careful design, the majority of these "vulnerable" components can be made to fail-safe, the equipment fail-danger fault rate can be kept low; especially as failures in many of the other components will have the same effect as a failure of the more active ("vulnerable") component in that particular stage or section of the equipment.

7. Since the validity of the prediction is dependent on the accuracy of the component fault rates used, it is important that as much information as possible should be collected on these fault rates. Ideally, the fault statistics used should be relevant to the environmental conditions appertaining at the location of the equipment concerned. In the absence of such specific fault data, the prediction can be completed using "basic" component fault rates which are as given in Table I for a typical land-based reactor, and multiplying these by appropriate stress factors. Table II is extracted from Reference 1 and gives the stress or K (multiplying) factors for general environmental conditions. As shown in the Table, components used in general purpose ground-based equipments have a K, factor of 1; this factor increasing to 2, 3 or greater dependent on whether the equipment is housed in a ship or in a vehicle travelling by road, rail or air. Other K factors can be used in the prediction to allow for components being used at higher or lower ratings and temperatures than those for which they were designed[1].

TABLE II

Component Stress Factors

General environmental condition	K, factor
Ideal, static conditions	0·1
Vibration free, controlled environment	0·5
General purpose ground-based	1·0
Ship	2·0
Road	3·0
Rail	4·0
Air	10·0
Missile	100·0

8. In a recent reliability assessment, the designer expressed doubt as to the accuracy of the failure rates attributed to metal bellows as used in control valves. Since many control valves were used in the system being assessed, and the bellows failure rate made a significant contribution to the fail-danger rate of the valve, it was evident that the confidence in the assessed value for the reliability of the control system was dependent on the accuracy of the bellows failure rate. An investigation was then made into their failure rates on an identical plant in the same factory. By searching through the maintenance records, it was found that twenty-four bellows had failed and been replaced in four hundred and fifty valve years of operation. This gave a bellows failure rate for that particular plant of $6/10^6$ hours, which compares well with the basic rate of $5/10^6$ hours as given in Table I.

9. Whilst it is convenient for the pressure switch example to consider all component failures as being either safe or dangerous, this can be an over-simplification especially where more complex equipment is used. As shown elsewhere[2], a more rigorous prediction would also take account of "neutral" faults and others giving only a slight shift in calibration. Furthermore, the fault category, which takes the form of a four letter code, would also signify whether the fault was "revealed" or "unrevealed" and if the former, which facility would indicate this.

EQUIPMENT FAILURE RATES

10. In the course of assessing the adequacy of automatic shutdown systems for several nuclear and non-nuclear chemical plants[3], predictions have been made of the failure rates of various mechanical equipments. A selection of these is given in Table III together with the

corresponding practically-experienced failure rates. As might be expected, there is less information available on the failure rates of large items of equipment than on the type of instrumentation equipment listed in Table III. This could stem from the growing demand for highly reliable shutdown systems and, consequently, the fault data relevant to them. Although the collection of this data does not in itself lead to improvements in the failure rates of individual equipments, it enables the designer/operator to demonstrate that the system reliability is up to the required standard, or, if not, to raise it to that standard by additional redundancy or more frequent proof testing.

TABLE III

Failure Rates of Protective System Equipment

Equipment	Failure rate faults/10^6 hours	
	Predicted	Practical
Pressure switch	15	16
Transmitting flowmeter	80	78
Pneumatic valve	22	29
Magnetic level switch	34	0 29 230
Differential pressure transmitter	51	87
Three term controller	*113 (68)	43

*Original prediction completed in 1964 using limited component fault data. The figure shown in brackets (68) is the failure rate that would result from using the component fault rates given in U.K.A.E.A. Report AHSB(S)R.117.

11. In the field of safety one is more concerned about fail-dangerous rather than *fail-safe faults*, but the latter are particularly irksome on power reactors and many other plants, since unscheduled shutdowns can be very costly. On one particular plant, many shutdowns were attributed to the protective system and it was decided to keep a log of the number of times that the protective system gave a spurious trip signal and shut down the plant. One object of this might have been to show that the cost of modifying the protective system - to reduce its spurious tripping rate - would have been more than offset by the consequent increase in plant production. For completeness, all plant faults were recorded. It was revealed by this study that only a small proportion of plant shutdowns were, in fact, due to faults in the protective system, the majority being due to failures of large machines, e.g., feed pumps, gas compressors, or failures in pipework.

12. As a result of this analysis and the unexpected information it produced, it was decided to record all equipment faults that occurred on three large important plants. The purpose of this was to identify the equipments that contributed mostly to the time for which the plant was non-productive. With this information to hand, it would then be possible to either rearrange or add to the existing equipment, so as to give greater plant availability. Over the past two years some 10,000 fault events have been recorded, some of which are still being sorted. From this and other sources, information has been collected on the failure rates of large items of mechanical equipment. Whereas the overall failure rate of protective instruments generally lies within the range of 0·1 - 1·0 faults/year, that of such items as boiler pumps and compressors appears - not unexpectedly - to be much higher. These range between 1·15 faults/year for boiler feed pumps and extend to 50 faults/year for high pressure, high powered gas compressors (including auxiliary equipment).

13. Fluidic devices are now being subject to reliability analysis in the U.S.A. and it is reported by Adler[5] that a test programme has been initiated to enable the reliability of these devices to be estimated. Tests have been conducted in which the influence of pressure, temperature and contamination upon the reliability of the devices has been studied. The devices used in the tests consisted of six five-stage registers, each register containing 25 digital elements. Although some information is given on failures, the tests made use of high

frequency pneumatic pulses (120 cycles/second). Hence, the apparent poor reliability, expressed in the mean time between failure of registers - which varied from three to ten days - was a high reliability in terms of the number of pulses correctly processed between failures (of the order of 10^9). It is the view of Adler that "probably the most important result of this phase of the reliability test activity was the discovery that all failures experienced in the test relate to a temporary loss of information". None of the failures was catastrophic, so component replacement was unnecessary.

14. In an example of a quantitative analysis of the reliability of a jet engine control system embodying fluidic devices, use is made of what is claimed to be one of the most useful tools for reliability prediction and design assurance, "the failure mode and effects analysis". The latter is, of course, the method applied to the prediction of pressure switch reliability previously in this report. The failure rates for the fluidic devices were taken from the test data and from other sources such as FARADA (FAilure RAte DAta programme sponsored and run by the U.S. Army, Navy, Air Force and NASA). For a fluid amplifier the failure rates vary between 0·01 failures/10^6 hours for external breakages, per connection, and 0·35 failures/10^6 hours for contamination of a 20 mil port. Using these and other failure rates, it has been calculated that the overall fault rate of a fluidic computer consisting of a dozen parameter control and logic units such as pressure ratio, speed and temperature, is approximately 260 failures/10^6 hours or 2·3 faults/year.

SYSTEM RELIABILITY

15. As discussed in the introduction, one of the purposes of calculating equipment failure rates is to enable the reliability of a system of equipments to be calculated. Such a system could be largely made up of the equipments listed in Table III, e.g. flow transmitter, pressure switch, pneumatic shutdown valve. Whilst only the overall failure rates of these have been given, it would normally be expected that the fail-danger fault rate would be not more, and often much less, than 50% of the overall fault rate; that of the pressure switch being some 20% of the total. To improve system reliability, it is the practice to make as many equipments as possible fail-safe on the loss of the pneumatic, hydraulic or electrical supplies.

16. By using redundancy and/or diversity in the sensing equipment, switching circuits and shutdown valves; and reducing the proof test interval, it is possible to attain a high order of reliability for a system. But, experience suggests[4,6] that it becomes increasingly difficult to reduce the probability of failure (to danger) when this gets down in the region of 10^{-3} to 10^{-4}. At this order of reliability, it becomes more difficult to substantiate many of the assumptions implicit in the simple mathematical model used in the numerical calculation of reliability, e.g., that the equipments are all working in their useful life phase, failures are independent, testing is perfect and repair is perfect. Hence, the chance of a common failure taking place, which can affect a whole family of equipments, becomes a distinct rather than a remote possibility. In one application the resilient seat rings of a whole series of valves suffered rapid deterioration when the temperature at the valves rose well above the design conditions. This occurred even though considerable care had been taken to limit the temperature to an acceptable value, the designers having been well aware of this problem in advance.

17. Where such items as pneumatic shutdown valves are arranged to fail-safe on the loss of supply and a minimum of two are used, there is normally little likelihood of a common fault affecting both valves. Even if the signal pressure lines were run in close proximity, most common faults would fracture the lines causing a safe shutdown action. There is the remote possibility, however, that the lines can be sealed off by a single common fault, thus preventing the air from being vented from the valve actuators and inhibiting a trip action. In an installation on one plant it was found convenient to run the pressure lines to the valve actuators across a walkway, alongside the process pipes. Although it was intended that a guard or cover would be erected over the pipes, this work was not completed when the plant was

commissioned. As can be seen from Figure 2, it would be a simple matter for someone to walk onto both pipes, which were run very close together, thereby sealing off the lines - one of the pipes had already been damaged in this way!

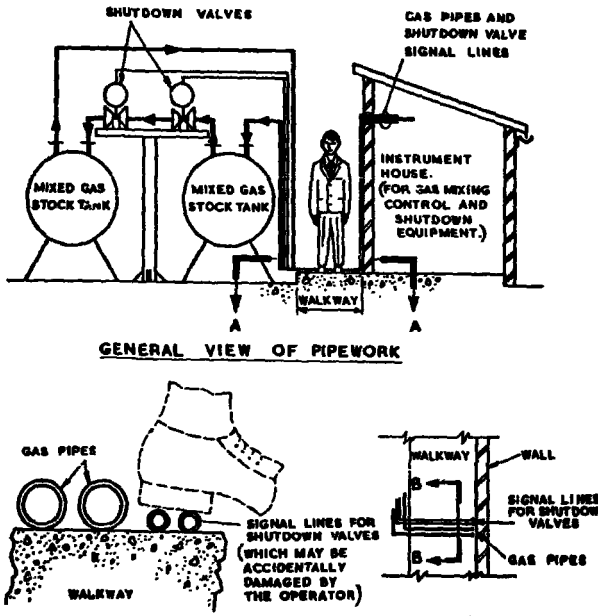


FIG 2 ARRANGEMENT OF SIGNAL LINES FOR PNEUMATIC SHUTDOWN VALVES.

18. To reduce the probability of common faults from inhibiting the correct action of a shutdown system, the system should be designed to conform with certain basic design principles[1]. One of these stipulates that, to retain complete redundancy between different equipments, the signal pipes (or cables) running to similar redundant equipments should have adequate physical separation. Had this principle been met in the above example, the probability of both valves being rendered ineffective by a single common fault would have been acceptably small in comparison with that due to their coincident failure because of random component faults.

CONCLUSIONS

19. By means of the method outlined, it has been found possible to predict the failure rates of mechanical instrumentation equipments. Provided that the component failure rates are known and also the environmental conditions likely to be met, it should be possible to extend this technique to much larger items of equipment, e.g., pumps, blowers, engines. Where several equipments are used to make up a highly reliable system such as a plant shutdown system, the overall reliability that can be achieved may be dependent on the frequency of common faults.

20. It should be borne in mind, however, that for the quantitative assessment of reliability to be meaningful, there is a prior need for the capability of the equipment or system concerned to have been shown to be adequate. This can be done by means of an independent safety assessment[1] in which the performance of the protective system is appraised, usually in terms of its accuracy and response, and compared with the response of the plant under all relevant fault conditions. When, by this method, the system is shown to have the required capability and to conform with the basic design principles, the "failure mode and effects analysis" becomes a most useful tool for predicting the reliability of mechanical instrumentation equipment for process control.

REFERENCES

1. GREEN, A. E., and BOURNE, A. J. "Safety assessment with reference to automatic protective systems for nuclear reactors". U.K.A.E.A. Report AHSB(S)R.117

2. EARLES, D. R. "Reliability growth prediction during the initial design analysis". Proc. 7th Nat. Symp. on reliability and quality control in electronics. Inst. of Radio Engineers, January 1961

3. EAMES, A. R. "Reliability assessment of protective systems". Nuclear Engineering, Vol. 11, No. 118, March 1966

4. HENSLEY, G. "Safety assessment - a method for determining the performance of alarm and shutdown systems for chemical plants". Inst. Measurement and Control, Vol. 1, April 1968

5. ADLER, A. R. "Reliability techniques applied to fluidic devices". Fluidic Feedbacks (The British Hydromechanics Research Association). Vol. 3, No. 4, April 1969

6. EPLER, E. "Common mode failure considerations in the design of systems for protection and control". Nuclear Safety, Vol. 10, January-February 1969

EUROPEAN NUCLEAR ENERGY AGENCY

COMMITTEE ON REACTOR SAFETY TECHNOLOGY

MEETING OF SPECIALISTS ON THE RELIABILITY OF MECHANICAL COMPONENTS AND SYSTEMS FOR NUCLEAR REACTOR SAFETY

Risø, Denmark, 24th-26th September 1969

SESSION I

A Theoretical Reliability Assessment of a Fire Protection System

by

S. Antocicco - CNEN
G. Tenaglia - CNEN
A. Valeri - CNEN

EUROPEAN NUCLEAR ENERGY AGENCY

COMMITTEE ON REACTOR SAFETY TECHNOLOGY

MEETING OF SPECIALISTS ON THE RELIABILITY OF MECHANICAL COMPONENTS AND SYSTEMS FOR NUCLEAR REACTOR SAFETY

Risø, Denmark, 24-26th September 1969

SESSION I

A theoretical Reliability Assessment of a Fire Protection System

by

S. Antocicco - CNEN
G. Tenaglia - CNEN
A. Valeri - CNEN

Introduction

In order to assess whether a system is adequate or not to the purpose it should be applied to, first of all it is necessary to define clearly the function the system is charged to perform and how long and under what stipulated conditions, the system is required to work. Just after that it will be possible to determine whether the considered system is able to perform the required function under the stated conditions, that is whether it functioning capability is adequate, and whether the system has the required attitude to keep such a capability for the required time, that is to say whether its reliability is adequate.

The reliability requirements are normally dependent upon both economic and safety considerations and in order to assist in the understanding of what is required and to permit logical thinking, the quantification

of reliability estimate is an important attribute. It is not just the value of the numerical expression which is salient but rather the information conveyed and the use made of such information. Furthermore, the limiting of subjectiveness helps to improve communication and reliability estimates carried out in a quantified fashion also lead to the constitution of criteria for the selection of courses of action which affect reliability. (1)

At the system level, it is almost impossible to have reliability data obtained or obtainable from the experience on the same systems already working under the same conditions. More usually the system, as such, to be analised is new and decisions have to be made at the "paperwork" stage. Therefore it is necessary to apply to some form of prediction. Generally speaking, as reliability data are most prolific at the component part level, the prediction methods are based on sectioning the system into elements of which reliability data are available and on determining what effects the various failure modes possible, of the above mentioned elements, produce to the all system performance. (2)

The amount and depth of statistical data needed for any analysis depend upon the characteristics of the system being analysed and also upon the requirements against which such a system is to be judged.

From the failure rate knowledge of the single elements into which the system has been divided, a reliability synthesis of system can be obtained by suitable mathematical modelling. (3, 4)

There are different prediction methods and each of them is a different approach to the same problem of making a reliability analysis.

Each of these methods differ from one another for the different basic assumptions that define the scopes, the characteristics and the limits of their application. In solving real cases, the choice of suitable method or methods must be done in verifying the adequacy of the basic assumptions to the real case.

It is not the intention of this paper to discuss any further the criteria that should lead in carrying out a reliability assessment of a system but to give an example of applied reliability analysis to a system made up mainly by mechanical components. The chosen example concerns a fire protection system installed in a laboratory for Plutonium handling.

System description

In the considered laboratory, Plutonium handling is carried out by operators in glove-boxes.

The rooms which contain such glove-boxes are protected against fire by two different systems. The first one protects each individual glove-boxes from fire which may start in the inside of it. The second one is a protection against fire which may start at the outside of the glove-boxes and against those fires which spread from the inside to the outside of the glove-boxes, in case the first fire protection system should not work efficiently.

Our examination will deal just with the second fire protection system; its main scope is to prevent the release to the outside of the laboratory of dangerous substances which might damage the neighbouring population.

The main function of the fire protection system is to introduce CO_2 in the room where the fire has started. From each room a group of CO_2 bottles has been provided, and located outside the laboratory.

The system can work authomatically, but allows at different stages the manual intervention from the part of the work staff or of the operators during work-time. In fig. 1, the main part of the considered system are shown schematically. Each room is provided with fire detectors, variable in number, according to the dimensions of the room itself. The fire detectors are of two different kinds.

In the case of fire in a room, one or more of them send a signal to a control panel which, by its term, immediately supplies optical and acoustic signals, and with a fixed delay, of a few minutes, operates the solenoid valve of the nitrogen servo control bottle related to the concerned room; such bottle is placed in the corridor in front of the exit door of the room.

The above mentioned delay allows the staff, present in the room where the fire took origin, to make the suitable arrangements to fight against it or to leave the place.

The nitrogen will be sent, by means of a piping, to the switching valve of the room and to two valves, called primary, allowing through CO_2, the opening of all the other valves of the bottles.

The outlet gas of the bottles is collected in suitable collectors, and conveyed to the main switching collector which sends it into the concerned room.

The bottles are placed in an individual system of automatic weighing; an alarm signal is provided in order to indicate decreasing in weight of about 20% for eventual self-discharge of the contained gas.

In the same time CO_2 is introduced, some operations are carried out, using the signal supplied by two pressure-switches: the first situated on the exit of nitrogen bottles and the second on the exit of the switching valve. The operations are the following: stopping of the fans which send the ventilation air to the rooms; closing the inlet air-lock in the concerned room, performing reduction of the suction air in all the rooms of the laboratory and closing the suction air locks in the concerned room; opening of an air-lock placed on the upper part of the room during the period of CO_2 intake in order to avoid a pressurization of the room.

In order to support all those operations which go on automatically, the plant staff can carry out the following interventions in case some parts of the system should fail to work; signaling to the central-panel, through push-button, of the presence of fire in the room; operating of the quick plant intervention, by the means of a device formed by a nitrogen bottle, with manual opening valve, situated near the first automatic control bottle; manual operating of switching valve and of the two primary valves on CO_2 bottles; and, in case of need, insertion, on the intake piping, of CO_2 drawn from a group of bottles relating to a room in which there is no fire, by the operation of the sectioning valves.

Reliability assessment

It appears clear that it is of no use to assess a system reliability, that is its ability to keep certain performance, if first one has not become sure that the system is able to perform in the desired manner, that is if the capability of the system has not yet been assessed.

Thus, also in the examined system the capability analysis was carried out before the reliability analysis. The result of such analysis has shown the adequacy of the system to the required function.

It is not the scope of our work to deal in detail with the analysis of the system capability. However we would like to hint at some aspects that have been particularly examined.

An accurate investigation has been made about the characteristics of the materials which could be involved in the fire; about the fire load in the room, about the quantity of air necessary to the combustion. Such investigation has made it possible to assess the adequacy of the detectors, particularly their sensitivity to the fire effects on which mostly the system sensibility depends; to ascertain that the right sensors have been placed in the right positions, and provided in a number sufficient to give an adequate detection threshold for the types of fire most likely to be encountered (5).

Besides, the assessment of the response of the system and the assessment of the rate of spread of the flame have been useful (in order) to judge whether the delay time between the fire detection and CO_2 inlet, was adequate or not.

Another aspect which has been examined concerns the role that can be played by the air-locks in case they should not work properly. Thus it has been made sure that both on the inlet and on the outlet of the ventilation, the malfunctioning of the only air lock or of the only fans, still allows an effective fire extinction. Moreover it has been ascertained that the CO_2 introduction system

and the quantity of CO_2 let in are able to saturate the room and that CO_2 is able to estinguish the fires caused by the materials contained in that room.

After having ascertained that the system is able to work as requested, it is possible to go on with the reliability assessment.

Such analysis could be done taking into account the failure of all the system components. However such method gives just a rough result which could be useful for example for maintenance purposes. In fact it is necessary to realize that the possible failures in a given system do not all cause the same consequences, therefore the probability of failures, dangerous to the desired operation, is less than the one which is obtained taking into account all the possible failures.

In our case, the first element of interest is the reliability of the automatic interventation of the fire protection system. The dangerous situations are caused by those failures which prevent the system from working, whenever requested to a fire. In order to get the probability of such dangerous situations, being not available failure rate information from previous operation of the system or similar systems, it is necessary to apply to a detailed study which takes into account all the possible system component failures. Once defined and classified the consequences of all the possible failures, it will be possible to individuate the dangerous failures in the above mentioned meaning. Once known the rates of the failure modes it is possible to calculate theoretically the system reliability parameters.

In a system of such kind in which the functioning request is casual, the parameter of most interest is the fractional dead time, that is the mean proportion of the total relevant time in which system is in the failed state. (6)

In fact, as the probability of getting a fire, which is not put out by other means, is a rather infrequent event and likely with constant rate of demand, the probability of a release of toxic products outside is given by the fractional dead time multiplied by the probability of getting a fire which is not put out by other means.

The fractional dead time is made up by two terms; the first due to unrevealed failures, and the second to the revealed ones. (2)

From an investigation of the failure modes of the system elements it has been found out that most failures are unrevealed and only a small part is revealed, which moreover, presents short repair-time and small failure rate. Therefore the calculation have been done neglecting the influence of revealed failures, as the term thus neglected is included in the incertainties inherent in calculations of such kind.

As to the calculation of the fractional dead time it is now necessary to know the expression of the function of the system failure probability, as such fractional dead time represents the mean failure probability with a fixed time interval between the successive system tests.

As to the calculation of the failure probabilities, the following basic assumptions have been made, which we think applicable in our case: failures are random, failures are independent, no compensating failures, testing time is negligible, repair of devices is perfect.

Moreover, a failure rate, constant in the time, has been used for all the components. In the case of mechanical components, we have thought it permissible, as it is reasonably to be supposed that during the plant life there should be no wear out because the various mechanical elements are not usually working. In such conditions the failure probability is calculated with the exponential function, and taking into account that the exponents are very small, we have used the approximate expression

$$P = \lambda \cdot t$$

where λ is the rate of a particular element expressed in faults/year and t is the test interval which in our case is 0.25 years.

As to the failure rates it has been used the values given in reference (2). Considering the fact that the system is installed in a nuclear research center, the standards of the devices, of their installation and maintenance, and the environment conditions have been supposed equal to those of which, the basic values shown in reference (2), refers to. Where necessary it has been taken into account the stress level of some mechanical components, introducing suitable K factors. Kfactor has been determined taking into account the following points: components are only operated occasionally; most of the system is not usually operated at pressure except during alarm condition; under conditions of occasional operation, the probability of sticking is greater; the gases used are clean so that blockage and sticking due to oily or dusty deposits are unlikely to occur; during the periodic checking the equipment is inspected to ensure that it is remaining in good condition.

In table I, the assumed failure rates and K factors are shown.

In fig. 2 we have shown the logic system diagram from the point of view of dangerous failures. The single block represent according to the cases single components or, as in the case of the electrical parts, group of components and devices for which a detailed reliability evaluation have been calculated previously. For each block the system function and the failure probability are shown.

The evaluation of the fractional dead time has been calculated using the NOTED computer program (7) and the result has been as follows:

$$D = 2.8 \times 10^{-2}$$

This value has been considered adequate referred to the reliability requirements made to the users. From the detail of the calculations it has been possible to notice that the greatest contribution to the total value is given by the switching valve ($0.65 \cdot 10^{-2}$), by the solenoid valve on the bottle of nitrogen ($0.65 \cdot 10^{-2}$) and by the control panel elements ($0.75 \cdot 10^{-2}$).

As to the last ones it is possible to suppose that the used value of the rate is sufficiently near to the real value because just a certain number of simple components are involved such as wirings and contacts of which the failure rate is known with some confidence.

As to the valves the rate is a value obtained from the average of data relative to valves with similar functions, but different realisations. As it is a question of complex components, a remarkable variability can be expected regarding the particular realization. In order to make sure that the real rates of the valves do not considerably exceed the utilized values a failure survey program of those valves has been arranged in agreement with the manufacturer.

As soon as a significant statistics is available, it will be possible to give a final judgement which will make it possible either to confirm the adequacy of the present system or to suggest the opportunity of modifications.

In our system, as it is possible to operate the system manually when the staff is in, it is of interest to calculate also the plant reliability taking into account the different manual interventions previously described. This implies the discussion of the human intervention reliability. In such a case there are difficulties of different kinds such as :

a) taking into consideration the environment and psycological conditions in which the staff will be operating during a fire;

b) the care requested for not customary operations;

c) the lack of guarantee as to the availability of the staff such as to make is sure an opportune intervention.

Notwith standing all that a fractional dead time calculation has been tried, supposing that the intervention of human operator is successful 9 times out of ten. Such rather low value has appeared to us reasonable, taking into account the literature data and all the above mentioned considerations. In the scheme of fig. 3, the dotted connections refers to manual interventions.

In this case it comes out that the fractional dead time is:

$$D = 0.74 \times 10^{-2}$$

mainly determined by the switching valve, (0.65×10^{-2}). The calculated value shows the positive influence of the manual intervention probability. However the human intervention is escluded from the

switching valve which, in such way, results to be the critical point of the system.

Since spourious CO_2 inlet, not preceeded by the optical and acoustic signals, could be dangerous for the staff, another element of interest is the knowledge of the rate of such an event in our plant.

The logic functional scheme of the system from the point of view of the spourious CO_2 inlets not signalized is shown in fig. 4.

The calculation has given the following value for the probability of spourious CO_2 inlet in a period of three months:

$$P = 4.8 \times 10^{-3}$$

As it can be seen, this value is mainly determined by the probability of leakage in the valves of nitrogen bottle, that is 5×10^{-3}.
The rate of spurious CO_2 not signalized is then:

$$1.9 \times 10^{-2} \text{ immissions/y}$$

The rate of spurious interventions preceeded by alarm have been calculated too and the obtained value has been:

$$0.15 \quad 1/y$$

CONCLUSIONS

The theoretical reliability assessment, carried out in a numerical way for the fire protection system, has shown how the switching valve is the critical point in the whole system and, comparing the results with the reliability requirements for the system, has allowed so far to judge the adequacy of the system even taking into account the existing uncertainties in the knowledge of the actual failure rates.

Since the theoretical assessment represents one of the initial steps in a performance evaluation and is of enhanced use if supported by practical results from actual field experience, a data collection system on the behaviour of the plant has been initiated with particular regard to those components which have been determined from this analysis to be critical from a reliability point of view.

REFERENCE

1 - GREEN A.E. Reliability prediction. UKAEA Report A.H.S.B. (S)R164 - 1969

2 - GREEN A.E. and BOURNE A.J. - Safety assessment with reference to automatic protective systems for nuclear reactors. UKAEA Report A.H.S.B. (S)R117 - 1966

3 - EAMES A.R. - Reliability assessment of protective systems. Nuclear Engineering - Vol. II No. 118 March 1966

4 - EAMES A.R. - The use of detailed fault analysis in evaluating fail-safe equipments. - UKAEA Report A.H.S.B. (S)R119 - 1966

5 - SAYER B. - Assessing fire protection systems. Business management - August 1967

6 - BOURNE A.J. - A criterion for the reliability assessment of protection systems. Control Vol. II - No. 112 - October 1967.

7 - WOODCOCK E.R. - The calculation of reliability of systems. The program NOTED - UKAEA Report A.H.S.B. (S)R153 - 1968.

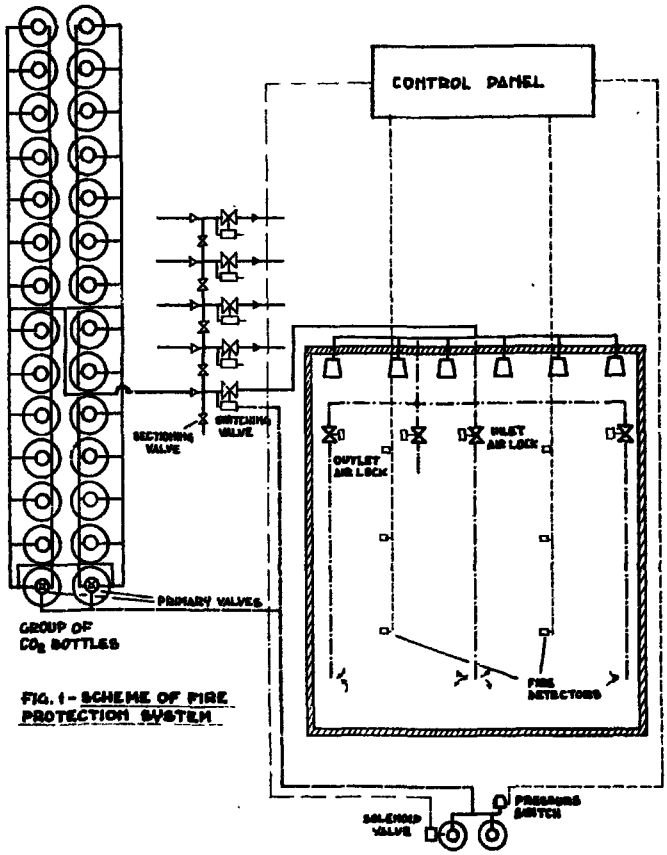


FIG. 1 - SCHEME OF FIRE PROTECTION SYSTEM

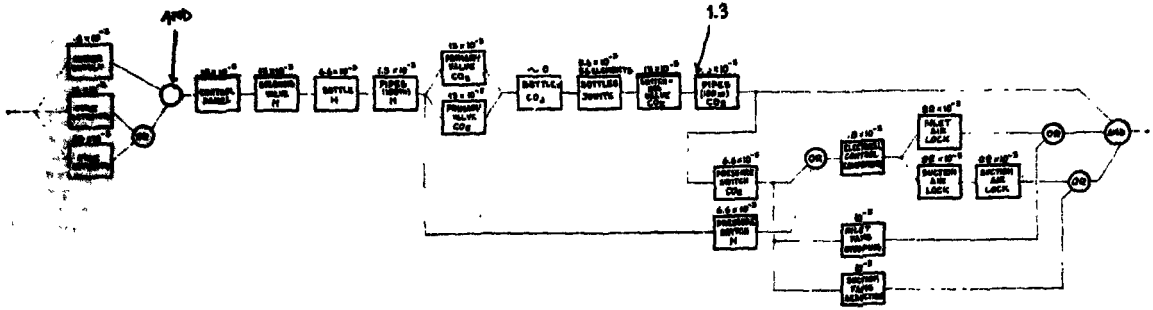


FIG.8 – LOGIC SYSTEM DIAGRAM
(AUTOMATIC OPERATION)

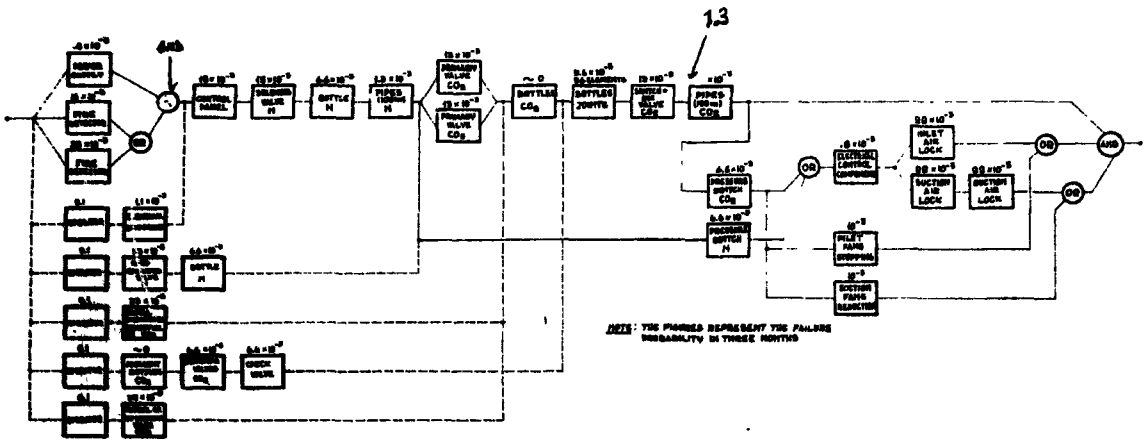


FIG.3 - LOGIC SISTEM DIAGRAM WITH MANUAL OPERATION

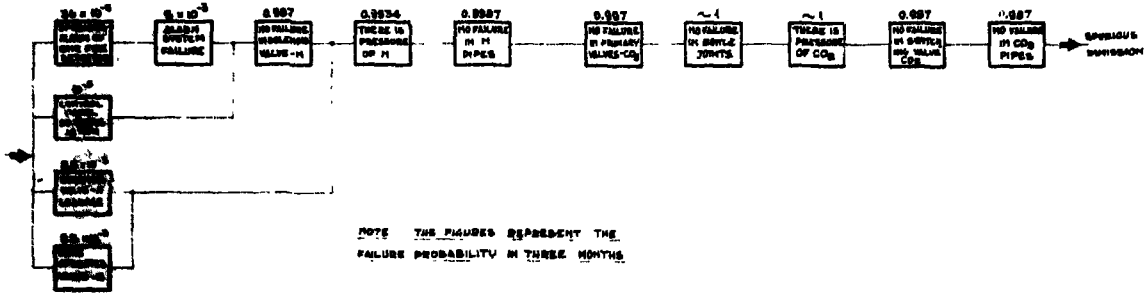


FIG. 4 - LOGIC DIAGRAM FOR SPURIOUS EMISSION

TABLE 1

Components	Assumed fault rate (% / kh)	K factor	Applied fault rate	Failure probability 3 months
Solenoid valve	3.0	0.2	0.6	13×10^{-3}
Bottle	0.3	1.0	0.3	6.6×10^{-3}
Primary valve	3.0	0.2	0.6	13×10^{-3}
Switching valve	3.0	0.2	0.6	13×10^{-3}
Pressure switch	1.5	0.2	0.3	6.6×10^{-3}
Air lock	0.1	1.0	0.1	22×10^{-3}
Hand operated valve	1.5	1.0	1.5	33×10^{-3}
Sectioning valve	1.5	0.2	0.3	6.6×10^{-3}
Check valve	1.5	0.2	0.3	6.6×10^{-3}
Manual operation valve	1.5	1.0	1.5	33×10^{-3}
Pipes	3×10^{-3}/m	0.2	0.6×10^{-3}/m	
Bottle joint	2×10^{-2}	0.2	4×10^{-3}	0.1×10^{-3}

Reliability and Availability of Two BWR Shut-Down Systems

by

P.K. Daublebsky and E.H. Koch

AEG Frankfurt

Germany

Paper presented on the ENEA / CREST Meeting

Risö 24. - 26. 9. 1969

Reliability and Availability of Two BWR Shut-Down Systems

by P.K. Daublebsky and E.H. Koch

Summary

The example of two realized scram systems is taken to show that a system that has to perform the same job on request simultaneously for many of independent customers (control rods), can be built more reliable and more economic, if a highly redundant network of components is used instead of a system composed of many independent blocks. This is true even if some of these customers need not be supplied.

The analysis showed that commonly used failure rates are too poor for the carefully fabricated and thoroughly controlled components of reactor stand-by systems.

In detail, it is pointed out to what extent system availability may be maintained by reduction of control time in the case that one component of a redundant system needs repair and the others are not available during test.

1. Introduction

In a boiling water reactor (BWR), the entire operational reactivity is controlled by control rods. With the present core configuration, 1 control rod is needed per 17 MW thermal power. This results in more than 100 control rods for a 640 MWe plant and nearly 200 control rods for a 1100 MWe plant which have to be hydraulicly injected within about 3 sec. in case of a scram.

In US BWRs and the former German ones, every rod is fitted with its own scram system (fig. 1), consisting of a pressure tank filled with water and nitrogen, of several valves and pipework and of the rod drive mechanism. With increasing reactor power, this system

becomes more and more intricate and voluminous since consisting of too many parts. Therefore, for the Würgassen power station a scram system is being built consisting of only six large pressure tanks, three of them discharging into a common ring header, and each of the two headers feeding every control rod drive. For a scram, water injection out of only two tanks is needed, the system thus having ample redundancy.

2. Reliability Analysis

For comparison, a system analysis was performed for both systems on the basis of the following assumptions:

1. A scram signal arrives correctly
2. Failure rates λ are independent of each other and independent of time (tested components, no wear and tear)
3. Reliability R is only a function of time,

$$R = 1 - e^{-\lambda t} \qquad (1)$$

4. Both systems are usually controlled every 8 weeks (vide [1]).

The functional diagram for the analysis of the former system is simple: All components of a subsystem for one control rod are arranged in series, and all subsystems are parallel and independent of each other. Therefore, from the failure probability of one rod, the failure probability of x rods is easily derived by use of the binominal distribution [2].

Fig. 2 shows a simplified version of the functional diagram used for the new system. The brief and handy time sharing program taken for the analysis is not able to handle a general network of components, but only parallel branches leading independently to success, with the exception of the fact that r out of n similar and parallel components or branches are required. Now the diagram shows that it is sufficient, if two of the three tanks (1) connected to either ring header (2) feed water through one of the two headers. The case

that only one tank per header works, had to be neglected. However, this case is negligible, since the probability of occurence per header is of the order F^2, if F is the failure probability of one tank, whereas the probability that no tank fails is of the order 1.

Failure rates were taken from the best sources available. A failure of a scram tank and the piping directly connected was regarded as a conditional probability: a mechanical damage has to occur, and the control instrumentation has to fail simultaneously.

The result of the analysis is plotted in fig. 3, failure probability of x rods vs. x. The dashed lines show the first outcome. Two points are significant:

1. The new system is by far better than the former one, if a limited number of rods is regarded. This is due to the high redundancy involved in the new system.
2. For the former system, the most probable effect predicted is failure of one rod. This is in contradiction to every experience and must be attributed to too pessimistic failure rates.

Now, failure rates were reduced by a factor of 10, those for piping and welds by a faktor of 100. The pipes are usually under reactor pressure of 70 bar, and they are only loaded by design pressure of about 150 bar during a scram.

The result is shown by the full lines. Failure probability of the former system appears quantitatively correct, however still worse than proven by experience. The scram systems of the reactors VAK, KRB and KWL (former design) have now been in operation for a total of ca $4{,}2 \cdot 10^6$ h (operation time multiplied by number of control rods). Prediction would be 7.8 failures. None was observed. With a confidence level aequivalent to 2σ, this means that system failure rate is up to now lower than the reduced one by a factor of 3. Therefore it appears justified to reduce common failure rates for application to mechanical reactor stand-by systems at least by a factor of 10.

Up to five resp. seven rods, the probability polygons of both systems have similar trends in fig. 3:
Failure probability is determined by the components without redundancy. For the new system, however, a simultaneous failure of about 5 rods is as probable as a breakdown of the entire system, the probability of which is given by a failure of both ring headers. This seems to be a disadvantage

of the new system. But the former system should behave equally, because a common mode will certainly underlie a simultaneous failure of some five rods and will then affect a lot of or all other rods, too.

At first sight, a failure probability for two rods of $5 \cdot 10^{-5}$ per scram might seem relatively high. It must be considered, however,

- that the result given in fig. 3 is still rather conservative, as already mentioned;
- that the plot is valid for the end of the control period of 8 weeks. For a system needed sometime within the control period τ, the average reliability

$$\bar{R} = \frac{1}{\tau} \int_0^{\tau} R(t)dt \qquad (2)$$

  is more representative, and this one is noticeably lower;
- that reactor conditions causing a scram, are only in very rare cases such that only one rod may fail (scram during start-up of the cold reactor);
- that in these cases not any two rods, but two defined rods have to fail, and this by itself reduces failure probability by about 4 orders of magnitude.

So we feel that the Würgassen system has reached a notably high level of reliability.

3. Availability Considerations

The overall plant availability shall be impaired as little as possible by subsystems such as the scram system. If as a consequence of failures detected the system reliability is too low, the reactor has to be shut down. Therefore minimum reliability should be maintained in some way, if one of the more possible failures should occur.

Water level and pressure control have by far the highest failure rates; repair should be possible without restriction in availability.

The same applies to the scram valves, the only active part in the system regarded.

For the former system, a high availability is given by the possibility to insert a rod mechanically by the control rod drive, if the scram mechanism should be found not working properly. Further reactor operation is possible when keeping this rod inserted, and tank or scram valve can be repaired when the usually open valve behind the scram valve is shut. The only penalty might be a restriction in reactor load towards the end of a fuel period.

With the new system, there is no equal possibility, because every tank feeds all control rods. Therefore surplus tanks must be installed to maintain the availability the former system had. Indeed, a sensitivity analysis of the new system proved among others that only four 50%-tanks, each equipped with two scram valves, are sufficient: If the thus reduced system is tested every 4 weeks instead of 8, failure probability will raise only by 10 %. So one tank of the three feeding in one header and the scram valves affiliated may be switched off for repair without reducing the reliability of the system or the performance of the reactor.

4. Influence of Control Time and Control Duration

Under the assumptions listed in paragraph 2, reliability of a component is equal 1 immediately after a successful control, and it diminishes as time goes on. So usually system reliability increases if control time τ - the time between two controls - is decreased. This may be used to maintain a required reliability of a redundant system, if one component needs repair.

Now, a new problem arose with an advanced version of the new scram system. It proved to be more economic and more reliable to furnish the system with four 100%-tanks, each equipped with one scram valve, instead of six 50%-tanks, each of them equipped with two scram

valves. During the test of a scram valve, which means to open the valve and shut it again, the tank is not available, because the motor operated check valve (fig. 1) has to be closed during the test in order to avoid a scram. This kind of test obviously means a reduction of the average system reliability, as defined by eq. (2); fig. 4 illustrates the fact. In addition, optimum average reliability may no longer be obtained for permanent control, but for a finite control time. An estimation of the influence is briefly given in the following.

A system be composed of n similar and parallel components, r of which are necessary for success, and R be the reliability of one component, $F = 1 - R$ its failure probability. Then the reliability R_s of the system is given by

$$R_{s(n,r)} = \sum_{\nu=1}^{n-r} \binom{n}{\nu} F^{\nu} R^{n-\nu} \qquad (3)$$

vide [2]. If eq. (1) is inserted and the resulting expression linearized, we have

$$R_{s(n,r)} = 1 - \binom{n}{n-r+1} (\lambda t)^{n-r+1} \qquad (4)$$

As fig. 5 illustrates, the reliability of a r-of-n system is reduced to that of a r-of-$(n-1)$ system during the test of the first component. If the test is successful, R_s jumps up to that of a $(r-1)$-of-$(n-1)$ system. It easily can be shown that the areas A_1 and A_2, being proportional to the system failure probability, differ by a factor of the order of the component failure probability,

$$A_2 / A_1 = O(F) \qquad (5)$$

Therefore it is sufficient to take account of the area A_1 or the respective largest. By attending to eq. (2) and (4), the average system reliability then results in

$$\bar{k}_s(n,r) = 1 - \frac{\binom{n}{n-r+1}}{n-r+2}(\lambda\tau)^{n-r+1} - \frac{t_0}{\tau}\binom{n-1}{n-r}(\lambda\tau)^{n-r} \qquad (6)$$

where t_D stands for the test duration. The expression obviously approaches a maximum for $\tau \to 0$, if the system is redundant ($n > r$); otherwise optimum control time is finite. (7)

Based on this theory, the influence of the test duration t_D on the reliability of the advanced four tank system shall be valued. The system be simplified to a 1-of-4 system with a total failure probability

$$\frac{4}{\tau}\int_0^{\tau}(\lambda t)^4 dt = 10^{-9}$$

in the average, which means $\lambda = 6{,}251 \cdot 10^{-6}/h$. If the components are tested successfully, the influence of t_D is negligible. But if one tank is found failed, the control time has to be reduced from $\tau = 56$ days to

$$\tau^* \approx 6 \text{ days if } t_D = 10 \text{ minutes},$$

$$\tau^* \approx 11 \text{ days if } t_D = 0 \text{ minutes}$$

if the reliability of the full system shall be maintained. Obviously the case that components are available during the test, is implied in the above theory if t_D is put zero. In a more general manner, this result is plotted in fig. 6. If the full system reliability (10^{-9}) is 10 times better than required (10^{-8}), the reduced control times will be:

$$\tau^* \approx 20 \text{ days if } t_D = 10 \text{ minutes},$$

$$\tau^* \approx 22 \text{ days if } t_D = 0 \text{ minutes}.$$

As a result of this paragraph, it may be summarized that also for the advanced version of the new scram system, the accumulators of which are not available during the test(lasting a few minutes),the required availability is guaranteed.

L I T E R A T U R E

[1] I. Bazovsky: Reliability Theory and Practice
1961 by Prentice - Hall. Inc.

[2] Kreyszig, E.: Statistische Methoden und ihre Anwendung
3. Aufl. Göttingen 1968

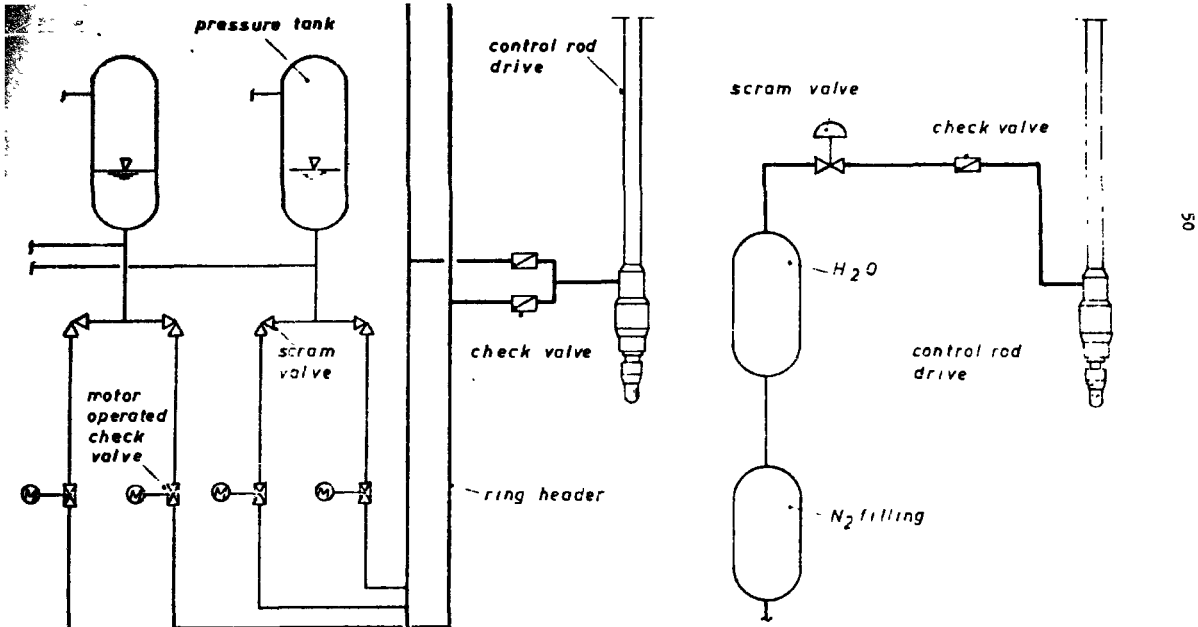
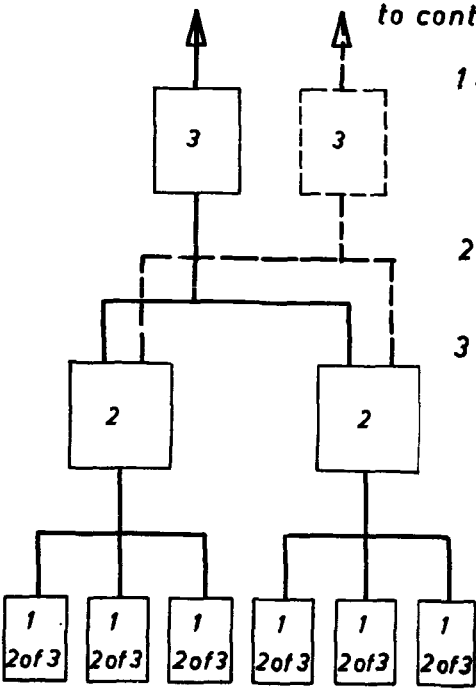


Fig. 1: Principle drawing of two scram systems

left: new system with few tanks and ring headers

right: former system with separate tanks



1 : Scramtank,
2 scramvalves
(in parallel),
2 checkvalves, piping

2 : ring header,
check valves, piping

3 : throttling valve,
check valves,
piping

Fig. 2: Functional diagram for system analysis of the new scram system

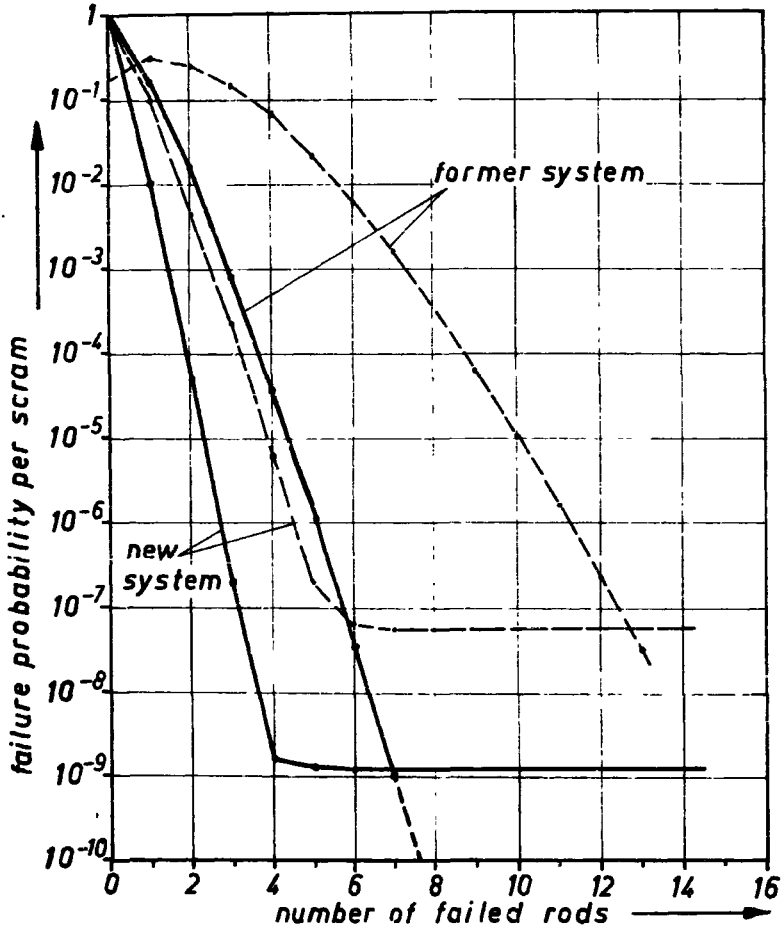


Fig.3: Failure polygon of the former and the new system for low rod numbers
Dashed lines : First outcome with conventional data applied to stand-by system
Full lines: Conservative result with improved data

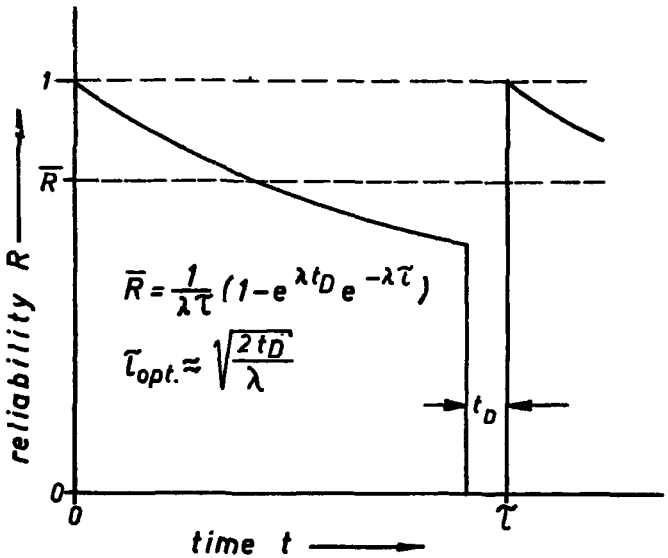


Fig. 4: Reliability R vs. time t of a stand by component with failure rate λ that is not available during test duration t_D. Average reliability $\overline{R}$ is optimized for for control time $\tau_{opt.}$.

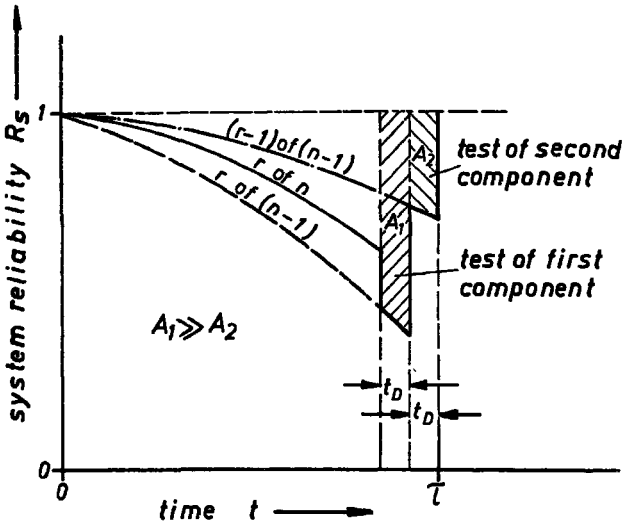
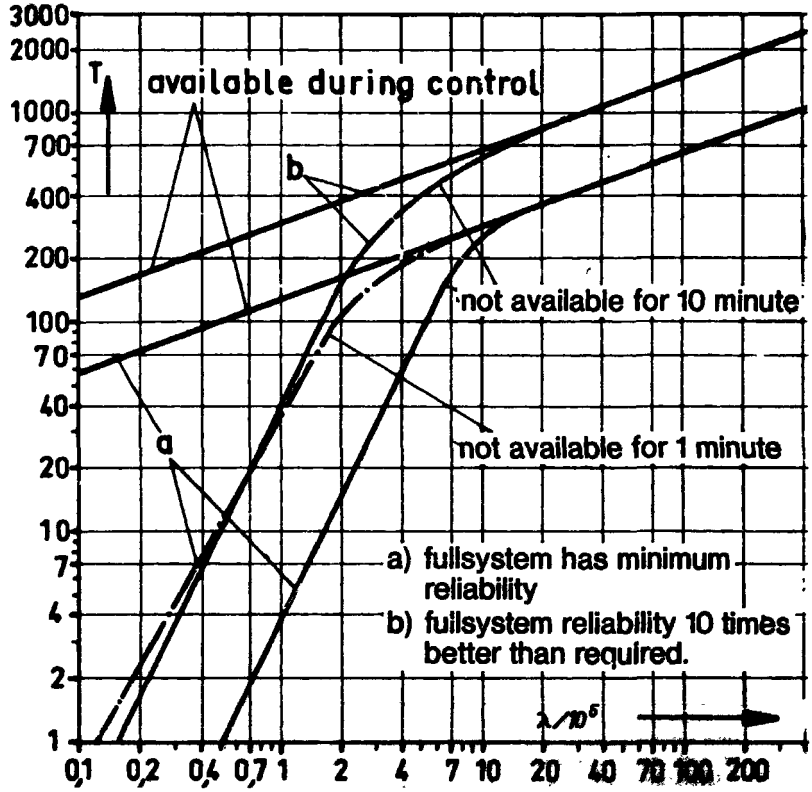


Fig.5: System reliability R_s vs. time valid for a system of n parallel components r of which are necessary. Components are not available during test duration t_D.



Reduced control interval T versus failure rate λ, plotted for a normal control interval of 8 weeks
1 of 4 components failed.

THIRD CREST MEETING OF SPECIALISTS
ON THE RELIABILITY OF MECHANICAL COMPONENTS AND
SYSTEMS FOR NUCLEAR REACTOR SAFETY

24th - 26th September, 1969. RISØ.

RELIABILITY ASSESSMENT OF A NOVEL LIQUID ROD SHUT-DOWN SYSTEM

S. Galli de Paratesi, L. Ghiurghi, H. Musik

Automation and Control Section

EURATOM, Joint Nuclear Research Centre, Ispra, Italy

Summary

A few pressure tube reactors have encountered difficulties in finding a suitable solution for the installation of safety rods and related mechanisms. This is because of the lack of available room in the reactor top and bottom spaces and the intricated inlet and outlet coolant tubes configuration.

To overcome these and other difficulties, special systems of liquid shut-down rods have been developed at the C.C.R. Euratom of Ispra, and a prototype system is now under completion. The studies have been carried out in the framework of Euratom D_2O development programs. The full scale prototype, which follows a feasibility mock-up, has been deemed necessary mainly for long term operation and reliability tests, before putting the system in actual service in whatever reactor.

Being this new system an emergency shut-down device, its reliability requirements cannot be overstressed. This paper is an attempt to predict the system reliability before any practical result can be drawn from the prototype exploitation. The prediction is based on published failure rate data for electro-mechanical devices. As imposed by available data, the exponential distribution is used throughout. Calculations will include fractional dead time for unrevealed and revealed faults and the relevant probabilities and spurious trip probabilities.

The numerical results of the prediction are intended as a preliminar evaluation, to be confirmed and/or completed with data gathered during the prototype operation and bench tests on components.

List of Symbols

D	fractional dead time
$F(t)$	$= P(T < t)$ probability of the device to fail in interval $0, t$
$f(t)$	$= \frac{dF(t)}{dt}$ probability density function of the lifespan of the device
$f_d(t)$	probability density of emergency shut-down demands
$p_1(\tau_c)$	*probability that the system will suffer one dangerous* failure within the period τ_c when it was thoroughly checked and without faults at time zero
$p_h(t)$	probability of a hazard arising by time t
T_f	mean failed time for all intervals
β	random emergency shut-down demand rate
λ	generic valve failure rate
λ_b	assumed failure rate for solenoid valve blockage
λ_j	flange joint failure rate
λ_s	assumed failure rate for solenoid valve spurious opening
τ_c	time interval between system overhauls
τ_r	time to repair a revealed fault
τ_t	interval between two subsequent valve routine tests
θ	plant spurious trip rate

Suffixes

r	revealed *system*
u	unrevealed system

1. INTRODUCTION

In 1966 a research activity on liquid rod shut-down systems was initiated in the frame of the ORGEL program, concluded at the end of 1968; it is now under way in the frame of the D_2O reactors assistance program. This activity has been given the name of EULER PROGRAM.

Research in this field is justified by the desirability of avoiding the difficulties that the installation of normal solid rods would raise in some reactor. In particular, in pressure tube reactors the installation of solid rods becomes extremely difficult, sometimes impossible, because the available space between the channel ends, above and below the core, is very limited. In addition, the fuel element loading and unloading facilities often prevent any other installation in at least one of the zones over and under the core, while the latter is sometimes inaccessible for high temperature reasons. Since liquid rods are essentially tubes of small diameter, in which a neutron absorbing solution is injected at the moment of the shut-down action, they easily fit the most complicated configurations and follow any path through the shield. Besides, all the drive mechanisms can be located in areas accessible for maintenance.

The studies began with the evaluation of several possible systems. Mock-ups were erected to test the feasibility and the dynamic performance of the two chosen systems called "bubble tube" and "gravity drop" type respectively. The goals of the mock-ups were achieved, and a completely instrumented full scale prototype of the "gravity drop" type is now under completion. The purpose of the prototype is not only to serve as a general test facility, before putting the system in actual work on a reactor, but also in particular for reliability studies and observation of long term performance of the component parts. It has been designed following the specifications imposed to the system which will actually be installed in a D_2O moderated pressure tube reactor.

The system being a fast acting emergency shut-down device for power reactors, no wonder that very much attention has been given to its reliable and safe operation. We will show the basic features that make the system very reliable from the reactor safety viewpoint. Then we will try to predict the interesting reliability parameters, i.e. fractional dead time, failure probabilities, spurious trip probabilities.

2. SYSTEM DESCRIPTION

The system is shown in Fig. 1. It is based on the principle of the U-tube, in a similar way to what has been done in some Canadian reactors with the "gas balancing system" to drop the moderator level in the case of emergency. In our case the application of that concept, proposed by the CISE (Italy), concerns small quantities of poisoning solution in independent in-core tubes instead of large amounts of D_2O in an annular chamber surrounding the calandria.

During the normal reactor operation, the neutron absorbing solution is

held out of the reactor core (at normal level) by means of a controlled differential gas pressure between the header tanks T-1 and T-2. Automatic fast opening valves V-1 through V-6, operated by means of a 2 out of 3 logic, are energized and closed, while the manual block valves upstream and downstream of the former are locked open.

Level control is performed through valve V-8, in a very simple way. That valve is open and injects a small quantity of gas into the rod system, via the header tank T-2, and into tank T-5. The latter is an auxiliary device, in parallel with the rods, in such a way that the liquid level in it is always the same as in the rods. The gas injected through V-8 is continuously transferred from T-5 to T-1, bubbling in the vertical connection pipe. If, for system leakage or upset, the pressure in T-2 drops, thus making the level in the rods and T-5 rise, the extremity of the bubbling tube is closed, so allowing the pressure in the rods to be restored at the set value, and the level will return to normal value. If, on the opposite, a system upset causes pressure in T-2 to rise, the level in rods and T-5 goes down, so causing the extremity of the bubbling tube (which is properly shaped) to open wider, allowing the discharge of more gas, until the normal level is restored. This kind of level control has proven very precise, and extremely reliable because no control loop is involved.

Shut-down action is performed by opening valves V-1 through V-6, and the rods are filled with solution up to the header T-2. At the moment of shut-down, valve V-8 is closed.

Each rod is part of an independent loop. An automatic stop valve is placed at the bottom (i.e. the lowest point) of each loop, valves V-9-1 through V-9-N. The bottom of each rod is connected also to a second, smaller diameter loop, the purpose of which is to circulate the solution by means of pump P_2 during reactor normal operation in order to prevent any possible deposit formation or disuniform concentration. The bottom of the circulation loops is also provided with valves, V-10-1 through V-10-N. After shut-down, by opening valves V-16, V-15, V-12 and V-9, the solution is circulated in the rods and through the solution tank T-3 by means of pump P-1, to prevent it from overheating by gamma irradiation in the in-core portion of the loop. Closing again all valves, the level controller can be re-energized and the rods withdrawn to their normal working level.

If required, the rods can be rinsed out before resetting the system. Of course, this operation requires the reactor to be put in a safe position by other means than the liquid rods, e.g. by lowering the moderator level or remove part of the fuel. The solution is discharged into tank T-3 by opening valves V-9, V-10, V-11 and V-15. Then valves V-11 and V-15 are closed, V-13, V-14 and V-16 opened and demineralized water is admitted to the bottom of the loops and discharged via T-2, V-16 and V-14 as long as required to clean the rods from the residual solution. Closing V-13, the system is then drained, and closing V-11, opening V-12, energizing V-1 through V-6 and the level controller, it can be refilled with solution by means of pump P-1. Once the normal level in T-1 is reached (level in the rod is automatically con-

trolled), the pump is stopped, all valves closed and the system is reloaded. Compressor C-1 takes care of gas pressure control, and keeps pressure in T-1 and T-3 near to atmospheric value, pumping into accumulator tank T-4.

3. PRELIMINARY CONSIDERATIONS

Preliminary qualitative considerations must be given before attempting a more rigorous approach, in order to point out the basic advantages of the system and where the reliability analysis must be centered.

Liquid rods consist of empty tubes, passing through the core, which are filled with a suitable solution every time an emergency shut-down is required. It is easily seen that this operation is by far easier and more safe than dropping a solid rod into a guide tube. In fact liquid rising in a pipe cannot stick to the walls, even if these are rough or rusted. Even a distorted or ovalized tube cannot prevent the correct shut-down. A frequent cause of dangerous troubles with rods, so simply does not exist in liquid rod systems, and this is a big advantage from a safety standpoint. Even the extreme case of an in-core pipe rupture (due e.g. to a pressure tube explosion) would not cause loss of safety. Of course, what would follow in that case cannot be considered a regular shut-down, because the moderator would be contaminated by the solution, but the reactor safety is still guaranteed.

Proper rod operation depends on gas pressure for level control. Loss of gas supply, whatever the reason, will always result in a spurious shut-down, i.e. in a safe operation. In fact, the driving force, being gravity, can never fail. As in the rest position of the system the rods are full of solution, one can hardly imagine an unsafe accident.

Really gravity driven solid rods share this property (apart from the possible rod sticking). Nevertheless, even though gas boosters could be simply designed in order to accelerate the shut-down action (which, in a sense, are similar to the accelerating mechanisms used in solid rods), liquid rods have the big advantage that they can be made faster only by increasing the gravity head and/or the ratio between the diameters of the vertical out-of-core pipes coming out of T-1 and the rod tubes.

Scram valves V-1 through V-6 are arranged, in order to increase the system reliability and allow on-line testing, in a 2/3 logic as shown in Fig. 2. Still, the safety channel instrumentation (sensors, trip amplifiers etc...) is out of the purpose of our work, so we will limit our considerations to the shut-down device itself. Valves V-1 through V-6 will be considered as the system's actuator, consisting of a series-parallel arrangement. These valves work in a fail-safe manner, i.e., they are closed when energised, for obvious safety reasons.

Finally, auxiliary equipment and circuits, as solution tank and pumps, helium compressor, flushing water lines etc., have no real bearing upon system safety. They work as separate systems, to perform auxiliary operations, and their malfunction cannot but impair the operation itself. These considerations will therefore be confined to the rod circuits proper, on both gas and the

quid sides. These circuits only consist of pipes and valves. The pipes being submitted to moderated temperatures and low pressures (the static head maximum), they are heavily derated, so that their failure rate can be neglected in comparison to the valves failure rate. For this reason we will henceforth only consider failures of valves and their combinations. Note that there is always a double barrier (a series of two valves) between the main loops and the auxiliaries.

4. FAIL-TO-DANGER FAULTS

4.1 Combined Revealed and Unrevealed Faults

We will begin our considerations on dangerous system faults with those caused by failures of valves at the bottom of the rods, i.e. valves V-9-1, 2, ...N and V-10-1, 2, ...N coupled with failures of valves in the auxiliary circuits. Faults in the former set of valves are revealed by means of probes placed just beneath each valve, to monitor the presence of liquid in portions of pipes which are normally dry. False opening or lack of internal tightness of valves V-11 through V-15, on the other hand, cannot be revealed because normally there is no liquid present at those valves, so that this kind of failure is of the unrevealed type.

Fig. 3 is a simplified diagram, showing the actual situation of the prototype system. The total number of rods is eight, six of which are enough to perform a correct shut-down, i.e. the entire system is faulty when at least three out of eight rods have lost liquid. Any rod has two valves through which solution could leak out, but liquid will not be actually lost unless at least one of the auxiliary lines, constituting the unrevealed system, is also open. Rod failures due to internal losses toward T-3 are therefore a combination of revealed and unrevealed valve failures.

From the general formulas of the majority vote schemes, the probability of failure of our revealed, three-out-of-eight system can be expressed as follows:

$$F_r = 1 - 28\, e^{-12\lambda_r t} + 48\, e^{-14\lambda_r t} - 21\, e^{-16\lambda_r t} \qquad (1)$$

The unrevealed system, consisting of three parallel lines, each one containing a given combination of valves, has the following probability of failure:

$$F_u = 1 - 4\, e^{-3\lambda_u t} + 7\, e^{-5\lambda_u t} - 5\, e^{-6\lambda_u t} + e^{-7\lambda_u t} \qquad (2)$$

A protective system failure can occur when both the revealed and the unrevealed systems are in the failed state at the same moment. If a revealed failure occurs first it will be immediately repaired, so that the only probability of significance of having a failure of the protective system as a whole is the occurrence of a revealed fault while at least one unrevealed line is in the failed state. Unrevealed type of faults include of course valve internal and external losses. Taking into account the repair action which takes place in a period τ_r and only considering the chance of having only one revealed failure

within τ_c, the probability of a system failure can be expressed by:

$$P_1(\tau_c) = \int_0^{\tau_c-\tau_r} dt' \int_{t'}^{\tau_c-\tau_r} f_u(t') f_r(t-t') \left[1-F_r(\tau_c-\tau_r-t)\right] dt \qquad (3)$$

being t' the time of occurrence of the unrevealed failure. The probability of having two system failures within the same period τ_c would be:

$$P_2(\tau_c) = \int_0^{\tau_c-2\tau_r} dt \int_t^{\tau_c-2\tau_r} dt' \int_{t'+\tau_r}^{\tau_c-\tau_r} f_u(t) f_r(t'-t) f_r(t''-t'-\tau_r) \left[1-F_r(\tau_c-\tau_r-t'')\right] dt''$$

being t'' the moment of occurrence of the second revealed fault. It is easily seen that $P_2(\tau_c) \ll P_1(\tau_c)$ so we can neglect it and all the successive ones.

For the assessment of the system fractional dead time, one must consider that, every time the system fails, it remains in the failed state for a period τ_r. Hence the mean failed time for all intervals equal to τ_c is:

$$\tau_f = \tau_r P_1(\tau_c) \qquad (4)$$

The corresponding fractional dead time for the period τ_c is given by:

$$D_1 = \frac{\tau_r}{\tau_c} P_1(\tau_c) \qquad (5)$$

For calculating $P_1(\tau_c)$ and D_1, the real problem is the value to be assigned to the valves failure rates, λ_u and λ_r. Published data do not mention important factors such as valve size, operation mode etc. In addition different sources often do not agree between each other. In these conditions suitable values must be in some way inferred.

The first consideration to be made is that it is quite reasonable to assume $\lambda_u = \lambda_r$. Secondly, the low pressure and temperature at which those valves are submitted, the absence of shocks, vibrations, fluctuations of environmental conditions, the fail-safe mode of operation, all suggest the choice of the most favourable data among the published ones, i.e. $\lambda_u = \lambda_r = 1.5/10^6$ h (Ref. 2). Assuming τ_c = 1 year, τ_r = 5 h, the results of the calculations performed by means of the ISPRA 360/65 IBM digital computer are as follows:

$$P_1(\tau_c) = 0.61 \times 10^{-7} \qquad (6) \qquad\qquad D_1 = 0.35 \times 10^{-10} \qquad (7)$$

It is perhaps worthwhile noting the importance of the excess rods included in the design. If, for instance, in the same project only one excess rod would be provided, the system would fail when two out of seven rods were in the failed state. In this case the probability of failure of the revealed system would be the only one which would change, would become

$$F_r' = 1 - 7\,e^{-12\lambda_r t} + 6\,e^{-14\lambda_r t}$$

and the overall system failure probability:

$$p_1'(\tau_c) = 0.15 \times 10^{-5} \qquad D_1' = 8.5 \times 10^{-10}$$

4.2 Revealed Faults of Flange Joints

Another source of dangerous system failures is the failure of flange joints at the rod bottom. This is a revealed type of fault, and the system again behaves as a three out of eight majority vote system. The fractional dead time for this case is given by:

$$D_2 = \binom{8}{3}(\lambda_j \tau_r)^r \tag{8}$$

where λ_j is the failure rate of each rod due to the flange gaskets at its bottom. The failure rate of a single junction is assumed to be $0.05/10^6$ h.

Each rod (Fig. 3) ends in two lines, and the liquid is only present down to the upstream side of the motorized valves, which are closed during normal operation, so that there are in total six wetted joints per rod. A fault of any one causes the failure of the rod, which means that $\lambda_j = 6 \times 0.05/10^6 \text{h} = 0.3/10^6$ h. Assuming again $\tau_r = 5$ h:

$$D_2 = 0.0025 \times 10^{-10}$$

4.3 Dangerous Failures Due to Scram Valves

Valves V-1 through V-6 form the system actuator. They are excited and closed during normal operation, and must open when shut-down action is required. There are three parallel lines, and a fail-to-danger fault arises when all lines (i.e. at least three valves in three different lines) remain closed upon emergency signal. Being these valves closed in normal operation, their sticking is an unrevealed type of fault. A sequential, weekly opening test (period $\tau_t = 168$ h) is planned for these valves.

The probability of a system failure due to this series-parallel arrangement is given by:

$$p(t) = (1 - e^{-2\lambda_b t})^3 \tag{9}$$

The relevant fractional dead time can be calculated by:

$$D_3 = \frac{1}{\tau_t} \int_0^{\tau_t} p(t)\,dt \tag{10}$$

From the usual sources, the assumed generic failure rate is: $\lambda = 4.5/10^5$ h. We estimate that in our case, where the valves are closed when power is applied to the electromagnetic motor and opened by a return spring, only 10% of the above value will contribute to valve blockage. The value to be used in

therefore $\lambda_b = 4.5/10^6$ h, which leads to the result:

$$D_3 = 8.6 \times 10^{-10}$$

5. PROBABILITY OF HAZARD

5.1 Shut-Down Valves

We will start the evaluation of the probability of hazard that arises where a shut-down is required while the system is in the failed state, by considering valves V-1 through V-6. The demand for emergency shut-down is supposed to be random and the corresponding demand rate β very low, in such a way that, for the valve test period τ_t, it can be said that $\beta\tau_t \ll 1$.

In this case, assuming $\beta = 4$ demands/year, the probability of hazard, at the end of the test period, is:

$$p_{h3}(\tau_t) = \beta\tau_t D_3 = 6.6 \times 10^{-11} \qquad (11)$$

At the end of a period τ_c comprising n weeks, the probability of hazard will be:

$$p_{h3}(\tau_c) = 1 - (1 - p_{h3}(\tau_t))^n \approx n\, p_{h3}(\tau_t) \qquad (12)$$

with good approximation. At the end of one year we will then have:

$$p_{h3}(1\text{yr}) = 3.4 \times 10^{-9} \qquad (13)$$

5.2 Block Valves at the Bottom of the Rods

A hazard can arise only when a demand occurs during the repair time of a dangerous fault. Hence, from (3):

$$p_{h1} = \int_0^{\tau_c-\tau_r} dt' \int_{t'}^{\tau_c-\tau_r} f_u(t') f_r(t-t') \left[1 - F_r(\tau_c-\tau_r-t)\right] dt \int_t^{t+\tau_r} f_d\, dt'' \qquad (14)$$

where f_d is the probability density of emergency shut-down demands which can be expressed as $f_d = \beta e^{-\beta t}$, and substituting in (14)

$$p_{h1} = (1 - e^{-\beta\tau_r}) \int_0^{\tau_c-\tau_r} dt' \int_{t'}^{\tau_c-\tau_r} f_u(t') f_r(t-t') e^{-\beta t} \left[1 - F_r(\tau_c-\tau_r-t)\right] dt \qquad (15)$$

Again assuming $\beta = 4$ demands/year and $\tau_r = 5$ h, it results $\beta\tau_r \ll 1$ and $1 - e^{-\beta\tau_r} \approx \beta\tau_r$. Calculating (15) by digital computer we get a probability at the end of one year of:

$$p_{h1} = 0.0062 \times 10^{-9}$$

6. SPURIOUS TRIPS

6.1 Shut-Down Valves

The reactor will undergo a spurious trip when at least one of the three lines connecting T-1 and T-2 (Fig. 2) is opened by spurious trip of the relevant valves.

The accumulated time to repair N faults is $T_f = N\tau_r$. The average number of faults occurring in a period T being $N = \lambda_s T$, it will be

$$T_f = \lambda_s \tau_r T$$

which is also the mean tripped time for one valve over a long period T. A spurious trip of a valve during the tripped time of the other valve of the same line will cause a spurious shut-down of the plant. Hence, the average number of plant shut-downs caused by each line during the period T is:

$$N_{SD} = T_f \lambda_s = \lambda_s^2 \tau_r T$$

The mean total spurious trip rate due to the three parallel lines is:

$$\theta_1 = 3 \frac{N_{SD}}{T} = 3\lambda_s^2 \tau_r \qquad (16)$$

Substituting the numerical values $\tau_r = 5$ h and $\lambda_s = 4/10^5$ h, which is the 9/10 of the assumed generic failure rate for solenoid valves (Ref. Chap. 4.3) it will result:

$$\theta_1 = 0.21 \times 10^{-3} \text{ trips/year.}$$

6.2 Spurious Trips through T-2 Overflow Line

T-2 overflow line is closed by valve V-16. This valve is normally closed, and its spurious opening while V-14 or V-15 have also opened by failure, will cause a plant spurious shut-down. The total failure rate of the system V-14, V-15 is $2\lambda_s$, hence the average number of trips over a long period T is $N = 2\lambda_s T$. The accumulated time to repair N faults is $T_f = N\tau_r = 2\lambda_s T\tau_r$. Since the rate at which V-16 produces spurious openings is also λ_s, the average number of spurious plant shut-downs is:

$$N_{SD} = 2\lambda_s^2 \tau_r T$$

The mean total shut-down rate results in:

$$\theta_2 = \frac{N_{SD}}{T} = 2\lambda_s^2 \tau_r \qquad (17)$$

Substituting the values already used to compute expression (16) one gets:

$$\theta_2 = 0.14 \times 10^{-3} \text{ trips/year.}$$

6.3 Spurious Trips Due to Level Control System

If T-5 and the pipes connecting it to T-1 get empty, a spurious plant shut-down would occur, because T-1 and T-2 would communicate directly. This can happen by V-7 spurious opening (Fig. 1) while at least one of the three auxiliary lines (the same set called "unrevealed system" in Fig. 3) has failed open.

The mean failed time over a period τ_c for the auxiliary lines is

$$T_f = \int_0^{\tau_c} p_u(t)dt \tag{18}$$

where

$$p_u(t) = 1 - 4\,e^{-3\lambda_r t} + 7\,e^{-5\lambda_r t} - 5\,e^{-6\lambda_r t} + e^{-7\lambda_r t}$$

or approximately

$$p_u(t) = 4(\lambda_r t)^2(1 - 1.25\lambda_r t) \tag{19}$$

Substituting in (18) and solving:

$$T_f = \frac{4}{3}\lambda_r^2\tau_c^3\,(1 - 0.94\lambda_r\tau_c) \tag{20}$$

When valve V-7 opens with the same failure rate λ_r during a failed period of the auxiliary system, a plant shut-down will occur, and the total number of trips per period τ_c will be $N = T_f\lambda_r$.
The trip rate is $\theta_3 = N/\tau_c$ and substituting N:

$$\theta_3 = \frac{4}{3}\lambda_r^3\tau_c^2\,(1 - 0.94\lambda_r\tau_c) \tag{21}$$

Being $\tau_c = 8750$ h and $\lambda_r = 4/10^5$ h :

$$\theta_3 = 3.8 \times 10^{-2} \text{ trips/year}$$

7. CONCLUSIONS

The analysis performed in the preceding chapters confirms what could be guessed through a qualitative inspection of the system, its properties, its behaviour under different circumstances (Ref. Chap. 3). The total fractional plant dead time, for all causes considered is:

$$D = D_1 + D_2 + D_3 = (0.35 + 0.0025 + 8.6)10^{-10} = 9 \times 10^{-10}$$

From this it is apparent that the major contribution to the system dead time is given by the scram valve system, while the contribution D_2 of the

losses through flange joints may be neglected.

The hazard probability p_{h2} is certainly negligible, so that it has not been calculated. p_{h1} and p_{h3}, representing independent events, may be added to give the overall hazard probability over a period of one year:

$$p_h = p_{h1} + p_{h3} = (0.0062 + 3.4) \times 10^{-9} = 3.4 \times 10^{-9}$$

The dominant part is, again, the scram valves assembly. It is perhaps useful to point out that the p_h calculated by us is only a part of the true plant hazard probability, (which should be, for instance, better than 10^{-5}, Ref. 5), because the consideration of the reactor safety instrumentation is beyond our scope. Nevertheless, a sound safety assessment should not be attempted without considering the influence of the safety chains, which may well play a major role.

Similar considerations apply to spurious trip rates. Of the various rates calculated, only one dominates by far, the loss of liquid from the level control system, which gives

$$= 3.8 \times 10^{-2} \text{ trip/year}$$

REFERENCES

1. Green, A.E. and Bourne, A.J., "Safety Assessment with Reference to Automatic Protective Systems for Nuclear Reactors." UKAEA-AHSB Report R117

2. Earles, D.R. and Eddins, M.F., "Reliability Physics (The Physics of Failure)." Proc. of the 9th Symposium on Reliability and Quality Control, S. Francisco, Cal., (Jan. 22-24, 1963), spons. by IRE, AIEE, ASQC, ASME

3. UKAEA-AHSB(S) R110, "Reliability Assessment by Fractional Dead Time."

4. Bourne, A.J., "Reliability Consideration for Automatic Protective System." UKAEA-AHSB Lecture No. 18

5. Final Hazard Report - Reactor WR-1, Canadian General Electric Co. Ltd. (1964)

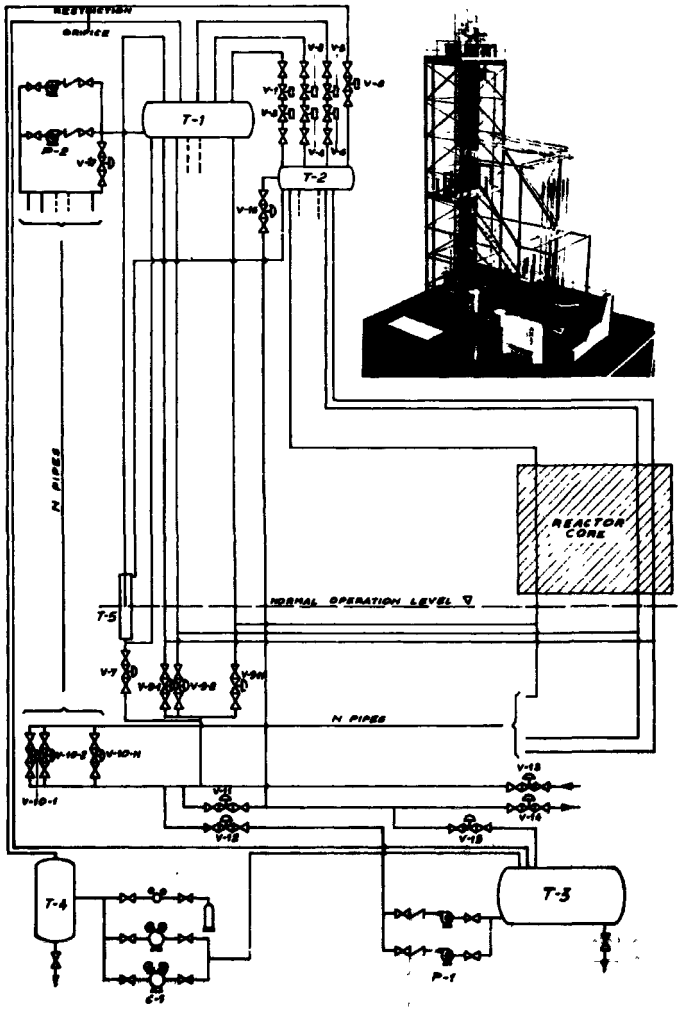


FIG. 1 - SYSTEM SCHEMATIC DIAGRAM

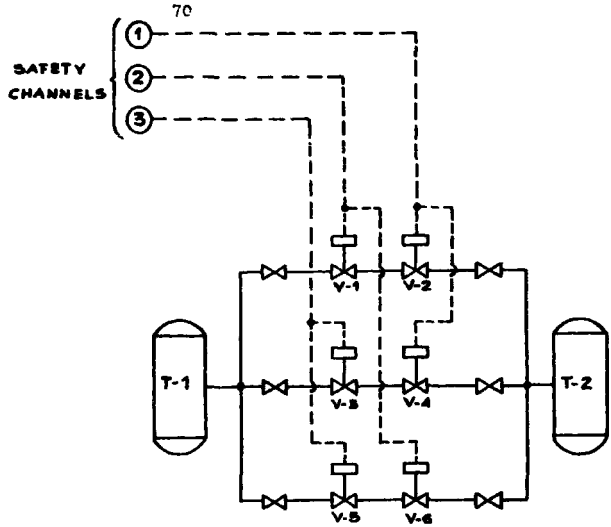


FIG. 2 - SHUT-DOWN VALVES ARRANGEMENT

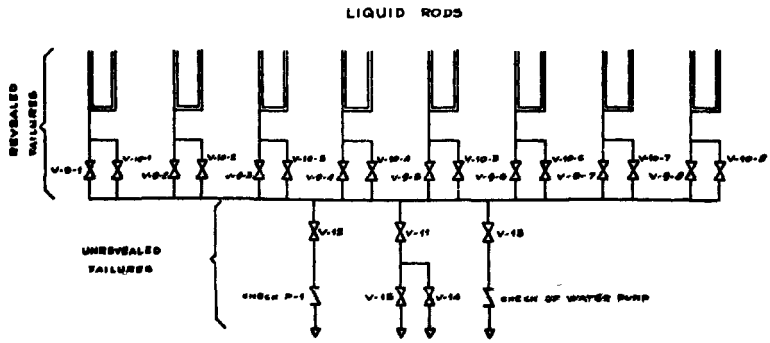


FIG. 3 - SIMPLIFIED SCHEME OF LIQUID LINES

For Presentation at the 3d CREST Meeting of Specialists on the Reliability of Mechanical Components and Systems for Nuclear Reactor Safety

Risø, Denmark, September 24-26, 1969

The Reliability of a Containment Isolation System

by

G. Mieze

Institut für Reaktorsicherheit

der Technischen Überwachungs-

Vereine e.V.

Köln, Germany

Abstract

The reliability of a containment isolation system is analysed and the results are compared to a reliability standard.

A short description is given of the analysed containment isolation system and related systems. The function of the systems is explained. The procedure of the reliability analysis is explained including failure effect analysis, development of the fault tree, selection of appropriate input data and the calculation of the overall system reliability.

The fault tree is calculated using a Monte Carlo method computer programme, which is explained to some extent. The results obtained from the computer are given and interpreted.

The overall reliability of the system is compared to a reliability standard. The derivation of that standard is explained and discussed.

The Reliability of a Containment Isolation System

1. Introduction

In the paper /1/ presented at the 2nd CREST meeting in Ispra an attempt was made to assess the reliability of an emergency power supply system. Several limitations of the problem were given due to our limited knowledge.

This paper shows the progress made in the assessment technique during the last year. A system analysis technique as well as a reliability analysis technique has been developed. Further, reliability computer programmes are now in use. In addition we have developed some idea of a reliability standard /2/ which also is included in this paper.

To demonstrate the recent developments the analysis of the containment isolation system of Kernkraftwerk Würgassen (KWW) has been choosen as an example.

2. Procedure of System Analysis

First of all, a reliability engineer has to translate the real design of a complex system into a reliability model of the system which can be subject to a reliability calculation.
In order to make such a translation a thorough knowledge of the design of the system and its functions is neccessary. Therefore, a system analysis must be performed in order to obtain this knowledge.
We have developed a system analysis technique which proceeds along the following items:

a) Analyse the design and the function of the system.
b) Define an undesired event and its criteria (fault criteria).
c) Define mission time, maintenance and test intervalls.
d) Perform failure mode and effect analysis.

We will now discuss in some detail the items defined above. The analysis of design and the function of system includes the following details. The location, the environment and the condition of operation are investigated and compared to the rated and design parameters. The system is also investigated for the possibility to bypass a failed component, for standby components and redundant components.

Certainly it requires thorough discussion of the system to produce a well-defined picture of that system.

Using the knowledge of the system obtained from item 1. one is able to define the undesired event of interest for which the probability is to be calculated. Now we will consider the example of KWW-containment isolation system. The undesired event is defined as:

Uncontrolled activity release in case of a reactor accident.

The activity might be released from the stack, to the air ventilation system or by direct leakage trough the containment shells.

The next step is to define the criteria of a failure of the system in order to define in occurences which lead to the undesired event. The criteria only may distinguish between the two states "operation" and "failure" of the system.

Applied to the KWW-system we obtain the following criteria:

a) System failure occurs, if the underatmospheric pressure in the gap between the two shells disapears.
b) System failure occurs, if activity release to the air ventilation system occurs and thus activity is released from the stack.
c) System failure occurs, if the atmospheric underpressure between the airlocks disapears.

These criteria are the basis of the reliability analysis.
The next step is concerned with mission length, maintenance and test intervalls.
Coming back to the example, the following periods are considered:

a) The possibility of unrevealed faults in the system in a test period. These faults might cause system failure at the next demand. Also the occurence of revealed faults is taken into account as the plant will probably not shut down after the event of a revealed failure.
b) Failure of switching over procedure from normal to accident operation.
c) Failure of System during accident operation.

The time intervals defined are test period of one year and 100 days of accident operation. The final step in the system analysis procedure is to perform the failure mode and effect analysis.

The failure mode and effect analysis deals with the failure modes of components and the consecutive reaction of system and subsystem following a failure of the component considered.
In case of the KWW-example the procedure used is as follows. The forms used are shown in fig. 1. For each component its name as well as its subsystem and its system must be entered. In addition the component function is required.
For some components the fail safe state should be defined. The columns of the form are entered with failure modes and its causes as well as the consequtive reactions of subsystem and system, i. e. whether the system has failed or not, whether it has lost redundancy or not, etc.

Using the informations worked out during the failure mode and effect analysis one can proceed to the important step, the reliability analysis.

3. Procedure of Reliability Analysis

After one has obtained a detailed knowledge on the system and its function the translation into a reliability model has to be carried out. To do this a

variety of methods has been developed, for example the fault tree method or the block diagramme meth . Also some sort of switch diagramme as well as reliability mapping methods are in use.

We found the fault tree method more convenient than the other methods. So the KWW example is worked using that method.
Due to some limitations of our computer programme, we are forced to separate the problem into three parts which are given by the three time periods defined in chapter 3. Always having in mind the indesired event the three cases we have are:

a) System is unavailable when demanded,
b) Failure of switching over procedure,
c) System failure during accident operation.

The fault tree method we use is already described in /1/.
Additional gates are defined to take into account a variety of data. In the following the signs and its functions allocated are explained.

System input

This input simulates an external system which already has been analysed or its failure probability is known from other sources. A name and a probability is assigned to this input.

Secondary fault

This input only is allowed with the secondary fault gate. A name, a probability and a repair time is assigned to this input.

Component input

To this input a component is assigned, defined by a name, a failure rate and repair time.

Standby gate

This gate is defined by only three inputs. E_1 simulates the component in operation while E_2 is assigned to the standby component. A failure of E_1 will cause the switch over equipment E_3 to actuate E_2. A failure occurs if either E_3 fails or E_2 fails during or after actuation.

Secondary failure gate

If a failure of component E_2 occurs a certain probability of a secondary failure of E_1 exists. So the output A simulates the secondary failure at component E_1.

In addition the wellknown gates "NOT", "AND" and "OR" are used

NOT AND OR

The number of inputs of AND and OR-gates are limited by the computer programme.

The first fault tree according to item 1 includes unreveald faults during test period as well as reveald faults which will be repaired during reactor operation.
The second fault tree treats the switching over procedure from normal to accident operation, i.e. the possibility of failure at the time of switching over.
The third fault tree takes into account the possibility of repair at certain components as well as secondary faults of the containment shells due tue failure of control etc.

This is the translation of the system into fault tree. The worked fault trees are not shown in this paper because they would blow up the paper to much.

The step that follows the fault tree preparation is the selection of appropriate failure rates and repair times. These data are also entered in the fault effect form. See chapter 3. The data situation has not much changed since last year, so I can drop an extensive discussion on that subject and refer to /1/.
The following four kinds of input data are used.

a) Probability of failure of an external system (for example power supply)
b) Secondary fault probabilities

c) Failure rates of components
d) Repair times

After one has selected carefully the failure and repair data, the input data for a computer run are prepared. The computer programme is described in chapter 4 and the interpretation of the results obtained is given in chapter 5.

4. The Ability of the Computer Programme

The Programme FESTVAR uses the MONTE CARLO Method and an importance sampling technique to reduce computer time. Its purpose is the calculation of an overall failure probability of the fault tree. In addition the critical failure combinations are given as a result.

Several asumptions are made in this version

a) Failure and repair are independent events.
b) The time of failure of components is random.
c) The time to failure is exponentially distributed.
d) The repair time is constant.

The qualitative limitations of this version are as follows.

a) Other than exponential failure distribution are not accepted.
b) Time response of components are not taken into account.
c) The system considered only may consist of components which might be "in operation" or "failed".
d) Exept the "undesired event model" no other reliability models may be treated.
e) All components must be allocated the same mission length.

The programme is able to handle the following inputs and gates

a) Components assigned with failure rate and repair time
b) Secondary failures
c) External systems which are input

d) NOT-gate
e) AND-gate
f) OR-gate
g) Secondary failure gate
h) Cold standby including the probability of switching over

The programme is also able to deal with loops in fault trees.

FESIVAR is written for a CDC 1604 computer and uses completely the available storage.

5. Interpretation of Results obtained

After the input data have been prepared a computer run is performed for each of the three fault trees. In the following the results of the computer runs are discussed.

5.1 System Failure at Normal Operation

Two types of failure might occur at normal operation

a) System failure due to a revealed fault of one or more components occurs and repair imediately takes place. During repair a reactor accident occurs, e.g. the system is not available.
b) System failure occurs if the system is called upon due to a reactor accident. This system failure is due to an unrevealed fault of one or more components.

The undesired event only occure if one of the above stated items holds. So the failure combinations obtained by the computer run neccessarily have at least two failure events, the reactor accident and one or more faulty components.

The most probable failure combination is the failure of the control-valve (34). During its repair a reactor accident occurs. The portion of this combination of the overall probability is about 60 %.
The occurence of the combined events failure of controller (12) and reactor accident and also of the combined events failure of the sensor (35) and reactor accident is less probable.

Their percentage of the overall probability is about 10 % and 27 % respectivly.

The results obtained are given in Table 1.

5.2 Failure of Switching Over

In case of an accident the system switches over from normal to accident operation, e.g. a reactor accident has already occurd and some signal has actuated the systems automatic. In this case no probability of successful operation per time but the probability of successful operation per demand is required. No repair is possible. The outcome of the calculation is as follows. Nearly all of the overall failure probability is given by two failure combinations, namely

the stack-valves (28) and (29) fail to close and
leckage-valves (44) and (45) do not open.

Its percentage of the overall failure probability is about 22 % and 78 % respectivly. The results obtained are given in Table 2.

5.3 Failure of Accident-Operation

In this case also the accident already has occured. In addition the system successful is switched over to accident operation. The occurrence of the undesired event is due to the failure of one or more of the components which result in system failure. The most probable failure combination is the failure of the control valve (34) and the motor-valve (20),e.g. the control of the system has failed. Its percentage of the overall failure probability is about 80 %.
Less probable combinations are failure of the sensor (35) and motor valve (20), and failure of the safety valves respectivly.
The possibility of a secondary failure of the containment is not reglectible.
The results are given in Table 3.

5.4 Overall Failure Probability

The results of the three calculations are

a) Normal Operation $F_1 = 2,5 \times 10^{-7}$
b) Switching over $F_2 = 4,1 \times 10^{-4}$
c) Accident operation $F_3 = 5,2 \times 10^{-3}$

As all three events are mutually exclusive, the overal probability of the problem is obtained by summation of the three single probabilities. So the probability of an uncontrolled activity release due to a failure of the containment isolation system is

$$P = 5,6 \times 10^{-3}$$

on the basis of an one years test intervall and 100 days accident operation.

6. Application of a Relative Reliability Standard

To derive requirement for the system reliability the overall risk of the plant is used. This is given by

$$R_1 = W_1 \times DL_1 \qquad (1)$$

where is

R_1 - Risk of MCA
W_1 - Probability of MCA
DL_1 - Damage level of MCA

The risk of MCA, R_1 requires the successful operation of the containment isolation system. At the event of the system failure the damage level will increase and thus, if the risk has to remain constant, the probability of the event MCA and failure of isolation system must decrease by the factor the risk increases.

If we have

$$R_2 = W_2 \times DL_2 \qquad (2)$$

where is

R_2 - Risk of MCA and failure of containment isolation system
W_2 - Probability of MCA and failure of containm. isol. syst.
DL_2 - Damage Level MCA and failure of containm. isol. syst.

and it is required

$$R_1 = R_2,$$

we obtain

$$\frac{W_1 \times DL_1}{W_2 \times DL_2} = \text{const.} \qquad (3)$$

where we have $W_2 = W_1 \times W_{CONT.}$. From this the unreliability requirement of the containment isolation system $W_{CONT.}$ derives

$$W_{CONT} = \frac{DL_1}{DL_2} \qquad (4)$$

The unknown in this type of reliability standard is the probability of the reference event and also the risk of that event.

Coming back to our example of KWW containment isolation system, both the damage levels in equation (4) have to be determinded. Therefore the accident of interest - loss of coolant - has to be analysed. In the following a brief description of the accident is given. In the course of a loss of coolant accident the pressure in the drywell of the pressure suppression containment increases and decays to the suppression chamber pressure at the end of the blowdown. The pressure will actuate the pressure supression system at a certain level. The system pressure is down at 0,1 atmospheric overpressure after a time of about 3 hours. During the course of the accident a portion of the actual fission products content of the core is released to the containment. With a certain leakage rate the fission products leak into the gap between the two containment shells, where the pumping system takes suction. If the pumping system operates successful the fission products are pumped back to the containment. Otherwise the fission products will be released into the

surroundings. In this case the following leakage modes are possible.

a) Leakage across the two containment shells
b) Release to the stack
c) Release to the ventilation system
d) Leakage of the large airlocks

Certainly a number of the modes will take place at the same time.

In case of successful operation of the pumping system leakage into the gap between the two shells is pumped back to the containment over a period of time of about 100 days. Then the remainder of activity is released carefully by the stack. A very rough calculation showed the damage level due to the failure of pumping system a factor 10 to 100 higher than the damage level due to careful release after the 100 days period. So the reliability requirement to the containment pumping system comes out to be about 10^{-2}. As already described in chapter 5 the actual probability of system failure is $5{,}6 \times 10^{-3}$, e.g. the probability meets the above stated requirement.

7. Discussion

In our experience the greatest difficulty is to translate the real system into an appropriate reliability model which can be calculated. This effort takes most of the time of the whole analysis. The analyst must reveal all functional interconnections, redundancies, standby functions as well as the possibilities of secondary failures and the influence of other systems and save them in a systematic way such that a complete picture of the system is designed. This picture should be checked by a second person to find out and discuss improper interpretations. In most of the cases this check has proved to be most effective.

From this system picture the reliability model may be derived. Again a check of an independent analyst is necessary in order to discover mistakes in the reliability diagramme. If the analysis is not performed with utmost care the probability of introducing mistakes might be higher than the probability of system failure.

The application of reliability standards requires in addition a good knowledge of the behaviour of the system and the reactor itself when an accident occurs. The course of accident might be different from that of the MCA. The reliability requirements must rely on the actual course of the accident.

Now, some remarks on the pumping system should be added. In this analysis a failure of the inactive components of the system such as piping is not incorporated. This is due to the fact that the failure rate of these components is very low. Also human error is not taken into account, e.g. operator error and poor repair. The reliability standard derived for the pumping system is obtained from a very rough calculation. Thus its accuracy is not known. But for demonstration of the method it will be good enough.

Cologne, 1st september 1969
mi/go

Appendix

Description of the Containment Isolation System

Operation at normal Conditions

The containment system consists of a double shell wall. The inner shell has to withstand the containment pressure. The gap between the two shells is held at an unteratmospheric pressure.
A system is provided to pump gas (which might be radioactive) from the gap either to the stack or to the inner containment. In the following we are concerned with that system. See Fig. 2.
One out of two installed compressors takes suction from the containment gap.and ,umps the air across a filter. One filter and one compressor are standby respectivly. The operating compressor is controlled by a bypass control system. The control system includes a sensor for differential pressure (containment gap-atmosphere) (35), a control unit (12) and a control valve (34). A motordriven valve is provided to close the bypass. That valve is actuated at the control room.
An aircooler is installed to cool down the bypassed pressurized air (12). The air cooler is controlled by the air temperature.
A measuring equipment for leak rate is provided at the pressure aide of the compressors. The normal way of the compressed air is along the valves (24, 25) and (28, 29) to the stack. The valves (24) and (25) are closed and valve (23) is opened. So the air is collected in tank (39) due to the closed valves (26, 27). Pressure and Temperature are measured in the tank. Valves (32, 32a, 33, 33a) and also valves (38, 38a) are closed. So no connection is made to the inner containment during normal operation. Further, leackpipes are provided to compensate the leckage of the valves and airlocks connected to the inner containment.
At normal operation the penetrations of the ventilation system of the inner containment are looked by two air locks in series. An inspection of the containment during operation is not planed.

Operation at Accident-Conditions
The systems purpose is agian to hold the underpressure against atmosphere in the containment gap. But the air sucked from the containment gap is pumped back to the containment.

The following activities have to be carried out to complete the switch over from normal conditions to accident conditions.

1. Both the stack-valves (28) and (29) must close
2. One of the two valves (30) and (31) have to be closed
3. The valves (32, 32a) or (33, 33a) have to be open
4. Valve (13) has to be open.

So the compressor will pump the air from the containment gap to the inner containment.

References:

/1/ G. Mieze and J. Eßmann, Reliability Analysis of an Emergency Power Supply System, 2nd CREST Meeting on Reliability Ispra, Italy, June 27 - 28 1968

/2/ O. Kellerwann, W. Ullrich, Probability analysis applied to LWR's, Application to the emergency core cooling system BNES Symposium on Safety and Siting, 28 March, 1969, London

/3/ Sicherheitsbericht KWW

/4/ Personall comminication AEG - IRS

Table 1

Unavailability of the Containment Isolation System in Case of an Accident

Set of Components failed	Percentage of Overall Failure Probability
Accident and Failure of the Control Valve (34)	60 %
Accident and Failure of the Pressure Sensor (35)	27 %
Accident and Failure of the Controller (12)	10 %
Accident and Failure of the Stackvalve (28)	0,5 %

Overall Probability of Failure $p = 2,5 \cdot 10^{-7}$

Table 2

Failure of Switching Over from Normal to Accident Operation

Set of Components failed	Percentage of Overall Failure Probability
Valve (28) and (29) fail to close	about 22 %
Valve (44) and (45) to open	about 78 %

Overall Probability of Failure $p = 4,1 \cdot 10^{-4}$

Table 3

Failure of Containment Isolation System at Accident Operation

Set of Components failed	Percentage of Overall Failure Probability
Control Valve (34) fails open and Motor Valve (20) fails to close	80 %
Pressure Sensor (35) fails and Motor Valve (20) fails to close	7 %
Vacuumbreakvalve (2) or (11) leaks extensivly	10 %
Controller (12) fails to operate and Motor Valve (20) fails to close	1,5 %

Overall Probability of Failure $p = 5,1 \cdot 10^{-3}$

Component: Page:

Subsystem:

System:

Function:

Fail-Safe Stage:

Failure Mode: Failure Cause:	Failure Rate:	Response of Subsystem	Response of System	Remarks

Fig. 1 Form of Fault Effect Analysis

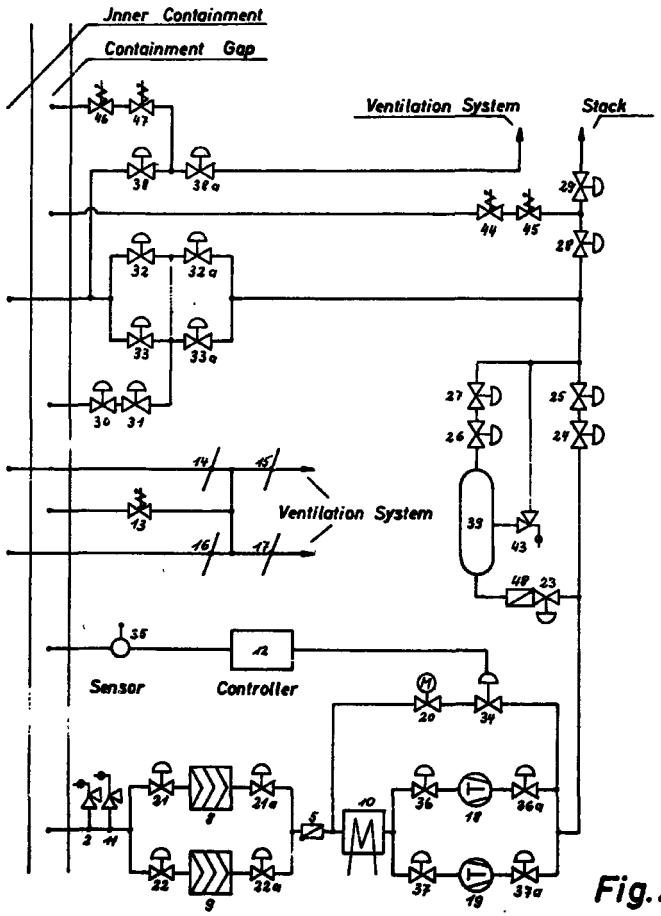


Fig. 2

Containment Jsolation System

17 093/1/III/69-E

Revised Issue

COMMISSION OF THE EUROPEAN COMMUNITIES

Directorate General
Industrial Affairs

INSTITUT FUR MESS- UND REGELUNGSTECHNIK

Laboratorium für Reaktor-
regelung und Anlagensicherung,
Garching

THE RELIABILITY OF EMERGENCY CORE COOLING SYSTEMS OF LIGHT WATER NUCLEAR POWER PLANTS

by

W. BASTL and H. GIESELER

Institut für Mess- und Regelungstechnik
Laboratorium für Reaktorregelung und Anlagen-
sicherung, Garching

H.A. MAURER

Commission of the European Communities,
Brussels

presented at the
Meeting of Specialists on the Reliability of
Mechanical Components and Systems for
Nuclear Reactor Safety

Risø, 24th - 26th September, 1969

SUMMARY

Two emergency core cooling systems installed in German light water power plants are described comparatively.

The functions of the different subsystems are discussed with respect to two examples of loss-of-coolant accidents on the basis of detailed flow schemes and reliability diagrams. The reliability of these systems is analysed and compared.

The study was performed by a digital computer programme.

Introduction

This study is the first step of a reliability investigation for Emergency Core Cooling Systems of Light Water Cooled Reactors. In the final stage, it is intended to combine extensive thermodynamic calculations regarding the cooling efficiency and the mechanism of accidents with the systems themselves which are designed to cope with these accidents. This is the only way believed to offer a chance for finally coming out with figures being really of some help in estimating the propability of a certain system to handle the accident in question.

Under this aspect, the main idea of the study presented here is not to give final results, but to show the difficulties which are involved when calculating the reliability of complex systems, and to bring into discussion the methods by which we tried to overcome these difficulties.

Emergency core cooling systems are installed in commercial power reactors to assure heat removal from the reactor core in case of a loss-of-coolant accident. The large range of possible rupture sizes up to the rupture of the main steam line in a BWR, or the rupture of a primary coolant pipeline in a PWR, results in different subsystems for each reactor, such as core spray systems, core flooding systems and depressurization systems.

This report presents two different emergency core cooling systems including their subsystems of 600 MWe light-water cooled power reactors currently designed to analyse the mechanical components of these systems and their cooperability from the point of view of reliability.

2. DESCRIPTION OF EMERGENCY CORE COOLING SYSTEMS

2.1. Emergency core cooling systems installed in a German 600 MWe Pressurized water reactor

The emergency core cooling systems are designed to prevent fuel melting and to limit the metal-water reaction to a negligible amount in the event of a leak in the primary system. The entire spectrum of possible leaks includes coolant piping ruptures up to the double-ended rupture of the largest pipe connected to the reactor pressure vessel.

For the analysed Pressurized water reactor, emergency core cooling systems, designed to cope with all possible loss-of- coolant accidents, consist of:

- the high-pressure water injection system,
- the recirculation system for residual heat removal, and
- a set of four accumulator tanks.

The primary purpose of the high-pressure water injection system is to supply boronated water to the reactor cooling system in case of a medium size pipe break (ND 125 ÷ ND 250). In this case, the system is designed to keep the whole core covered. Four

high-pressure pumps are installed in the circuit, but the capacity of two pumps is sufficient to cope with this accident. The four pumps are working on two parallel pipelines so that, in case of a rupture of one of these lines, an automatic switch over to the other line is possible without endangering the core. The system will be activated by a coincident low-level and low-pressure indication in the pressurizer. If the pressure in the primary cooling system decreases to the operational pressure of the accumulator tanks (2o at overpressure) the tanks will work in addition.

In the case of a double-ended rupture of the primary coolant pipe (ND 700), the reactor would loose its coolant in about 10 sec. The melting of fuel cannings and fuel elements can, in this case, only be avoided if the core is reflooded after about 200 sec. This means that about 60 m^3 water are to be fed into the pressure vessel by the four accumulators. Each accumulator has a capacity of 2o m^3 so that one unit can be considered as stand-by unit. At the same time, together with the accumulators, two of the four pumps of the resudual heat removal system work with a capacity of about 500 m^3/h each. To remove the decay heat from the core, a water capacity of about 500 m^3/h is necessary. If the whole capacity of the four boronated-water storage tanks of 56o m^3 is fed into the reactor pressure vessel the pumps of the residual-heat removal system will take suction from the containment sump and operate via the heat-exchangers in a closed circle with the primary system.

Summary description

High-pressure water injection system:

number of loops	: 2 (1)(*
pressure range of operation	: 110 ± 20 atm
number of pumps	: 4 (2)
flow rate per pump	: 250 m^3/h (at 30 atm)
method of activation	: low-level and low-pressure indication in the pressuriser
emergency coolant source	: 4 (3) boronated water storage tanks with a capacity of 200 m^3 each

Pressurized accumulators:

number of loops	: 4 (3)
type of water storage tank	: gas pressurised, on line
pressure range of operation	: up to 20 atm
capacity of the accumulators	: 4 x 20 m^3
method of activation	: check valve opens when accumulator pressure exceeds system pressure

Recirculation system for residual heat removal:
(system injecting water at low pressure)

number of loops	: 2 (1)
pressure range of operation	: 8 atm overpressure to atmosphere pressure
number of pumps	: 4 (2)
flow rate per pump	: 500 m^3/h
method of activation	: low-level and/or low-pressure
number of heat exchangers	: 2 (1)

(* The numbers in brackets indicate the number of circuit components necessary for full capacity operation. The numbers without brackets give the number of components installed.

2.2. Emergency core cooling systems installed in a German 600 MWe Boiling water reactor.

The emergency core cooling systems of the analysed Boiling water reactor include an automatic depressurization system, a high-pressure water injection loop, and a core flooding system as well as a core spray system. The automatic depressurization system consists mainly of six primary system relief valves (of which three are necessary for full capacity) which open to the wetwell at reactor overpressure and after closing of the pressure emergency penetration valves, enabling thus core cooling by the low pressure emergency cooling systems. They start operating automatically at 78 atm overpressure below the designed pressure of the primary system valves. The valves also remain open below the closing pressure, when signalled to do so, after a loss-of-coolant accident. This signal is based on simultaneous signals from

- high drywell pressure,
- reactor scram because of low primary water level,
- non-operation of the feedwater system,
- non-operation of the emergency core cooling system.

The high-pressure water injection loop is designed to feed water into the reactor vessel under loss-of-coolant conditions within a reactor pressure range of 89,5 to 12 atm. absolute at a rate of 900 t/h. The system consists of one steam turbine driven pump, arranged outside the pressure suppression system in the reactor building. The cooling water is supplied from the wetwell and is pumped into the feedwater line.

A low water level in the reactor will start automatically loop operation when the primary pressure is above 78 atm absolute, and a high reactor water level will stop it. If the pressure in the primary system drops to about 17 respectively 15 atm the core spray system or the core flooding system respectively is automatically activated at a certain water level. The core spray

system consists of two independant loops. Each of the two pumps is designed for a capacity of 800 t/h at 17 atm. The core spray loops will spray water onto the top of the core so that the water will flow down the fuel channels and cool the fuel by radiation and steam convection. The core flooding system is designed to reflood the core up to the top of the jet pump diffusers which means 2/3 of core height. This will be possible because the core shroud is sealed circumferentially around the vessel wall. The maximum capacity of the core flooding system at pressure equalization of the primary circuit and the pressure suppression system will be 4.200 t/h. Four pumps are installed in the system but only three of them are necessary to reach full capacity. If the water level of 2/3 of core height is reached only one pump is required for long-term maintenance of level and cooling.

Another residual pump is necessary to fill the suppression pool with water from the sump.

The normal feed water pumps are not considered in the reliability calculation.

Summary description

Automatic depressurization system:

number of relief valves	: 6 (3)(*
operating pressure	: 78 atm, overpressure

High-pressure water injection loop:

number of loops	: 1
number of pumps	: 1 (steam turbine driven)
pump flow rate	: 900 t/h (pressure not known)
pressure range of operation	: 89,5 to 12 atm, overpressure
method of activation	: low reactor water level

Core spray system:

number of loops	: 2 (1)
number of pumps	: 2 (1)
flow rate per pump	: 800 m^3/h (at 17 atm overpressure)
pressure range of operation	: from 17 atm overpressure to pressure equalization of the primary circuit and the pressure suppression system
method of activation	: low reactor water level and low reactor pressure
emergency coolant source	: wetwell or sump of drywell

Core flooding system:

number of loops	: 2
number of pumps	: 4 (3)
flow rate per pump	: 1 400 t/h at 6 atm and 800 t/h at 19 atm
pressure range of operation	: from 15 atm overpressure to pressure equalization of the primary circuit and the pressure suppression system
maximum flow rate of the whole system at pressure equalization	: 4 200 t/h
emergency coolant source	: wetwell or sump of drywell
method of activation	: low reactor water level and low reactor pressure

(* The numbers in brackets indicate the number of [illegible] necessary for full capacity operation. The numbers without brackets [illegible] the number of components [illegible]

3. RELIABILITY DIAGRAMS

The reliability of the two Emergency core cooling systems (ECS), as described above, is calculated by a digital computer programme*) with respect to two cases of accidents:

a) rupture of a minor line, e.g. the connection to the pressurizer or smaller leakages in the main lines of the primary coolant system;

b) rupture of a main line of the reactor primary coolant system.

Depending on which of these two cases happens, different parts of the ECS are involved. As a consequence of large ruptures, a quick depressurisation occurs and a large amount of coolant is lost. In that case, the low-pressure system, layed out to restore the lost water within a short period of time, has to handle this accident.

For smaller ruptures, however, the problem is to feed water into the reactor vessel against high pressure. Here, the high-pressure injection system has to operate properly or one has to take care for an artificial depressurization of the reactor vessel so that low-pressure feeding systems can be used.

As regards reliability calculations, the systems under consideration involve the following problems:

a) they consist of different subsystems which are operating subsequently.
b) the subsystems are overlapping, e.g. they use partly the same lines for equipments.

To overcome these difficulties, the line as shown below was followed in our calculations:

- if subsequent actions are necessary to cover the accident under consideration they are supposed to appear simultaneously;
- if the same equipment is used by different subsystems they are introduced only once to the reliability diagram, although they have to work in fact subsequently according to the operation modes;

*) The programme used is Reliag, written in FORTRAN IV

- if special valves have to be operated during one operating stage (active), whereas they have to remain only in a certain position during the other stage (passive), they appear in the diagram twice, together with the corresponding failure rates.

3.1. Pressurized water reactor

3.1.1. Rupture of injection line

To calculate the reliability of the ECS, a rupture of one injection line is postulated (Fig. 1). In comparison to the rupture of the pressurizer line, in this case too one of the two feeding branches for the ECS is lost.

According to the lay-out, two subsystems of the ECS are necessary to handle this accident:

- the high-pressure water injection system (HS);
- the low-pressure water injection system (LS).

Therefore, in order to calculate the total reliability for sufficient cooling when a break of one injection line does occur, the HS and the LS are combined with and "AND"-gate (Fig. 12).

3.1.1.1. High-pressure water injection system (HS)

The redundancy of the storage tanks for the boronated water (3 out of 4) and the high-pressure pumps (2 out of 4) is verified in the diagram (Fig. 5). Assuming a rupture of one injection line, the corresponding valve TJ 31 will close automatically so that feeding into the ruptured line is prevented. Therefore, starting at this point in the diagram, only the second feeding branch is available for cooling purposes. This is shown in the diagram by logical "AND"s.

3.1.1.2. Low-pressure water injection system

When the pressure has decreased to 20 kg/cm^2 the accumulators start to feed into the reactor vessel. Below 8 kg/cm^2 further cooling is achieved by the LS. As the accumulators need not be operated in this case they have not been incorporated into the diagram (Fig. 6).

On principal, two pumps (for one residual heat exchanger each) are started regardless the fact that one of them is feeding into the ruptured line. Two pumps serve as stand-by units, one for each line. Considering the accident as defined above, only one half of the LS is available for further cooling. Therefore, a 1 out of 2 redundancy is taken into account for the pumps and only one line as a connection to the HS.

Finally, the suction lines are switched over from the storage tank to the sump. The lines and valves used for this operation are introduced in the diagram in series.

3.1.2. Rupture of one main coolant line

For the reliability calculation, a rupture of the hot leg of one main coolant loop is assumed. The following subsystems are involved with this accident:

- the accumulator system (AS);
- the low-pressure water injection system (LS).

Therefore, the reliability of the AS and the LS is combined with and "AND"-gate to take into consideration the fact that both systems have to operate properly in order to handel the break of one main coolant loop (Fig. 12).

3.1.2.1. Accumulator system (AS)

In case of the rupture of a main coolant line, the pressure of the primary system is decreasing so rapidly that the HS need not be used for sufficient cooling. The set point of the AS is reached quickly, and the accumulators start to feed water into the reactor vessel. Because of the rupture, one of the four accumulators is feeding into the defect line. For the second one, it cannot be excluded that its cooling efficiency is very low because of the short circuit via the reactor. The remainir two accumulators are both necessary to provide enou cooling fluid for covering the first phase of the accident. This fact is considered by using a 2 out of 2 system in the reliability diagram (Fig. 7).

3.1.2.2. Low-pressure water injection system (LS)

As regards the LS, the considerations are valid as given in chapter 3.1.1. Again, one feeding branch is not available due to the rupture. Therefore, the same reliability diagram can be used as before (Fig. 6). However, when taking into account the connection line between AS and LS (incorporated into the HS for the previous investigations), the corresponding tubes and valves are added in series at the end of the reliability diagram for the accumulator system (Fig. 7).

3.2. Boiling water reactor

3.2.1. Minor rupture in the primary system

This accident is characterised by a comparatively slow loss-of-coolant so that the first step for cooling the core has to be achieved whilst the reactor is on full pressure.

The following subsystems of the ECS are designed to handle such accidents:

- the depressurization system (DS);
- the high-pressure water injection system (HS);
- the core spray system (SS);
- the core flooding system (FS).

According to the layout of these subsystems, either one of the high-pressure systems (DS or AS) and the core spray and/or* core flooding systems have to operate. The associated logic diagram is given in Fig. 13.

3.2.1.1. Depressurization system (DS)

This system consists of 6 remote controlled pressure relief valves which have a 3 out of 6 redundancy (Fig. 8).

3.2.1.2. High-pressure water injection system (HS)

The reliability diagrams show two lines; one line for the turbine (including pipes and valves) which has to drive the injection pump (Fig. 9(1)), the other one for the pump itself and the associated injection facilities (Fig. 9(2)). In order to calculate the reliability for the total HS, these two lines are to be taken in series.

3.2.2.3. Core spray system (SS)

The system is laid out with a 100 % redundancy. One pre-selected loop is started automatically in case of emergency. The other one is in stand-by condition. This is shown in the reliability diagram by combining the two branches with an "OR"-gate; switching over to loop 2 is taken into account by "ACT" (Fig. 10).

3.2.1.4. Core flooding system (FS)

In the first phase, the core is flooded by three pumps, the fourth pump is in stand-by condition.

* see table 2 - possibility of improvement

This is verified in the reliability diagram (Fig. 11(1)) by a 3 out of 4 system with an "ACT"-block in the forth line.

Starting with the point where these 4 systems are leading into two parallel lines (which have to operate both for sufficient cooling), the diagram shows a 2 out of 2 logic combination. Assuming the rupture in one feeding line, somwhere after the check valve L 45, the total coolant has to pass valve L 69 and the damaged line has to be blocked by closing the valves L 43 and L 51 (Fig. 4). This is taken into account by incorporating the acting valves into the diagram and by considering only one connection line to the reactor vessel (Fig. 11(2)).

During the second phase, only one of the four pumps mentioned above is used for flooding, a second pump delivers water from the sump into the suppression pool in order to refill it. Bearing in mind that in this stage two different suction lines are in operation (Fig. 4), the remaining two pumps are to be seen as redundant equipments according to a double 1 out of 2 system (two 1 out of 2 systems in parallel). Looking at the reliability requirements for the systems regarding phase 1 (3 out of 4) and phase 2 (double 1 out of 2), there is no doubt, that the former are the more stringent ones. Therefore, in calculating the total reliability of the two phases of operation, a 3 out of 4 system is introduced in the reliability diagram. The double 1 out of 2 system-stage is omitted. Only the additional pipes and valves which are necessary to operate phase two are taken into account: the two sump-suction lines as a 1 out of 2 system and in addition the line for refilling the suppression pool (Fig. 11(3)).

3.2.2. Rupture of recirculation line

As a consequence of this accident, a rapid depressurization of the primary system does occur. Therefore, the high-pressure cooling systems need not operate. In this case, the core spray and/or* the core flooding system (phase 1 with associated pipes and valves of phase 2) have to operate. The reliability diagram for this case is shown in Fig. 13.

4. DISCUSSION OF RESULTS

The tables 1 and 2 show the reliability values of the emergency core cooling subsystems and of the two cases of accidents for the German 600 MWe Boiling and Pressurized water reactors discussed. The reliability as function of time was calculated for an inspection time of 400 hours, except for the depressurization system of the BWR the reliability of which was assumed as an average value over 2 years (normal reactor shut-down period). The failure rates, shown in the reliability diagrams, were taken from the literature.

A comparison of the two high-pressure water injection systems (HS) shows that the one of the PWR is only for about 0.5 % more reliable than the system of the BWR. The reason lies in the 2 out of 4 system for the HS of the PWR in opposite to the 1 out of 1 system of the BWR. On the other hand, a 100 % redundancy exists for depressurizing the reactor vessel of the BWR because of the depressurization system (DS) which is not installed in the PWR. Due to the few components and the 3 out of 6 concept, the depressurization system of the BWR has a very high reliability.

The core spray and core flooding system for the BWR correspond to the low-pressure water injection and accumulator system for the PWR. The reliability values of these subsystems show that the SS of the BWR is the most reliable subsystem of the low-pressure cooling systems, due to the 100 % redundancy (99,998 %).

However, a distribution effect of the spray nozzles and the cooling

* see table 2 - possibility of improvement

mechanism could not be considered in the analysis; only the availability of cooling water above the core has been taken into account.

The core flooding system for the BWR has a lower reliability value (99,45 %) since it consists of a 3 out of 4 system. Due to the 2 out of 4 concept, the LS of the PWR has a higher reliability than the FS of the BWR (99,72 %). In spite of the 2 out of 2 concept of the accumulator system (AS), the reliability amounts to a value of 99,84 % because it consists of fewer components.

Whilst the reliability values of the subsystems of the ECS for the two reactors show some differences, a comparison of the reliability, calculated with respect to the two cases of accidents, shows that the probability for sufficient cooling, when both, rupture of a main coolant line or rupture of a minor line, do occur, is nearly the same. The difference of about 0.1 % is very low.

The calculation was performed for comparative reasons under the assumption that for the BWR, in case of a rupture of the injection line, either one of the high-pressure systems and both core spray and core flooding system have to operate while, in case of a rupture of the main coolant line, both, core spray and core flooding system, have to operate to cope with the accident.

The availability of the emergency core cooling systems installed in a BWR can, however, essentially be improved when, in case of a rupture of a main coolant line, each of the two subsystems, core spray or core flooding system (SS or FS), can handle the accident. For this case

R_{RM} (400) was calculated to be R_{RM} = 99,99994 %.

A similar arrangement of duplicate cooling facilities is possible in case of a rupture of the injection line. In this case, one of the two high-pressure cooling subsystems (DS or HS) and one of the two low-pressure cooling systems (SS or FS) must operate to cope with the accident.

R_{RI} may improve to R_{RI} = 99,9998 %

Following this discussion, one can imagine already the many conflictive situations that arise when attempting to compare the two ECS's. There is no doubt that this kind of investigation is useful to find weak points in the design or in looking for the best solution regarding safety- and economical considerations for important subsystems. However, to get real reliability figures as wanted by the safety engineer or by the evaluater, and this brings us back to the introducing remarks, it is necessary to even better define the kinds of accidents, to take into consideration the thermodynamic efficency of the ECS's and to include investigations of the consequences for the development of the accident, when assuming the one or the other subsystem should fail.

Table 1: Reliability of ECS for PWR

1. High-Pressure Water Injection System (HS)

$$R_{HS}(400\ h) = 99{,}81\ \%$$

2. Low-Pressure Water Injection System (LS)

$$R_{LS}(400\ h) = 99{,}72\ \%$$

3. Accumulator System (AS)

$$R_{AS}(400\ h) = 99{,}84\ \%$$

Rupture of Main Coolant Line

$$R_{RM}(400\ h) = R_{LS} \cdot R_{AS} = 99{,}55\ \%$$

Rupture of Pressurizer Line

$$R_{RP}(400\ h) = R_{HS} \cdot R_{LS} = 99{,}53\ \%$$

Table 2: Reliability of ECS for BWR

1. Depressurization System (DS)

R_{DS}(mean value of 2 years) = 99,999998 %

2. High-Pressure Water Injection System (HS)

$R_{HS}(400\ h)$ = 99,32 %

3. Core Spray System (SS)

$R_{SS}(400\ h)$ = 99,998 %

4. Core Flooding System (FS)

(Phase 1 including sump and suppression pool pipes and valves)

$R_{FS}(400\ h)$ = 99,45 %

Rupture of Main Coolant Line

$$R_{RM}(400\ h) = R_{SS} \cdot R_{FS} = 99{,}45\ \%$$

Improvement

$$R_{RM}(400\ h) = R_{SS} + R_{FS} - R_{SS} \cdot R_{FS} = 99{,}99994\ \%$$

Rupture of Injection Line

$$R_{RI}(400\ h) = R_{SS} \cdot R_{FS}(R_{DS} + R_{HS} - R_{DS} \cdot R_{HS}) = 99{,}45\ \%$$

Improvement

$$R_{RI}(400\ h) = (R_{DS} + R_{HS} - R_{DS} \cdot R_{HS})\ (R_{SS} + R_{FS} - R_{SS} \cdot R_{FS}) = 99{,}9998\ \%$$

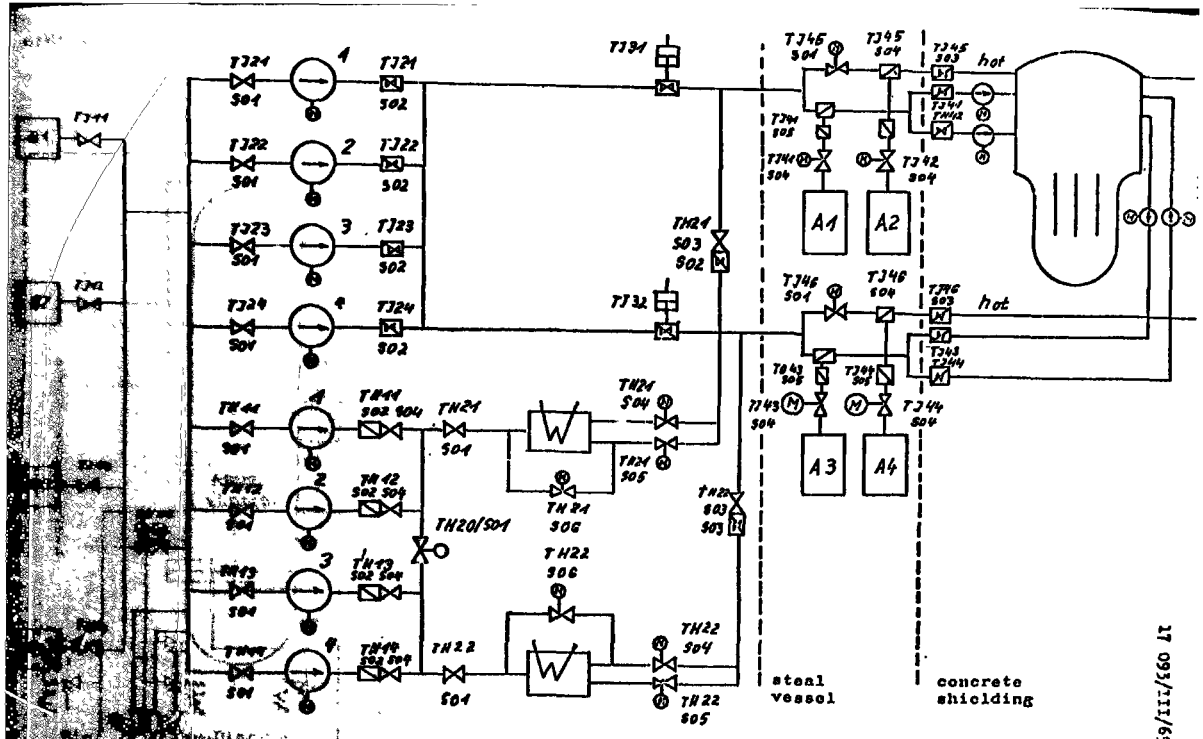


Fig. 1 Flow-Diagram of the Emergency-Core-Cooling-System for PWR

Fig. 2 Flow Diagram of the High-Pressure-Water-Injection-System for BWR

Fig. 3 Flow-Diagram of Core-Spray-System for BWR

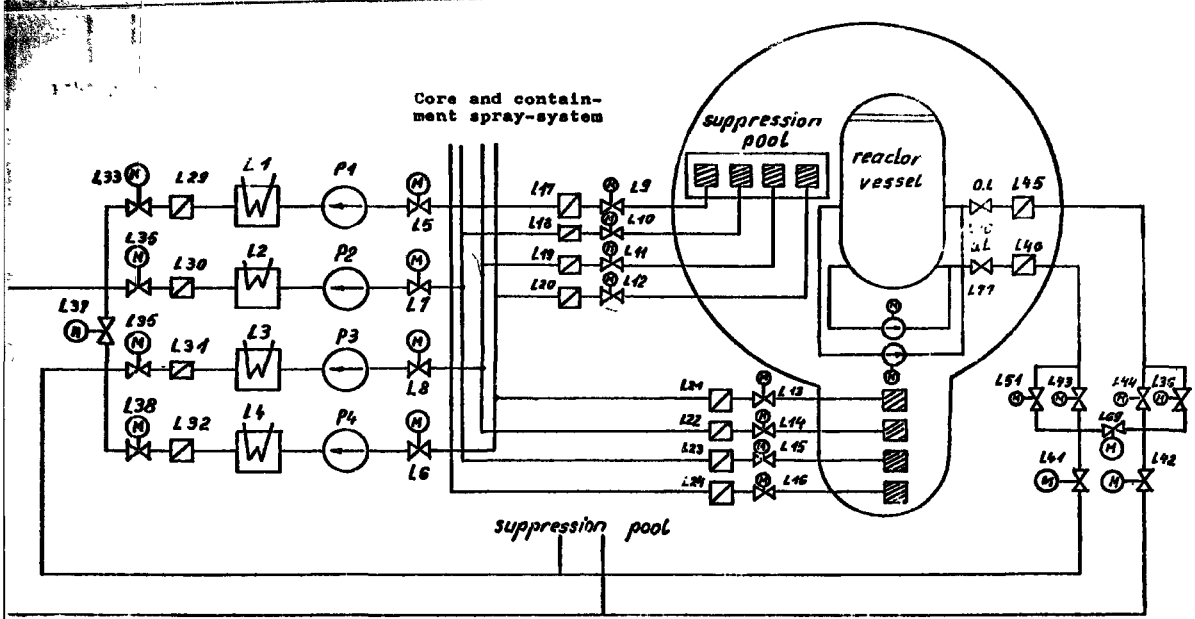
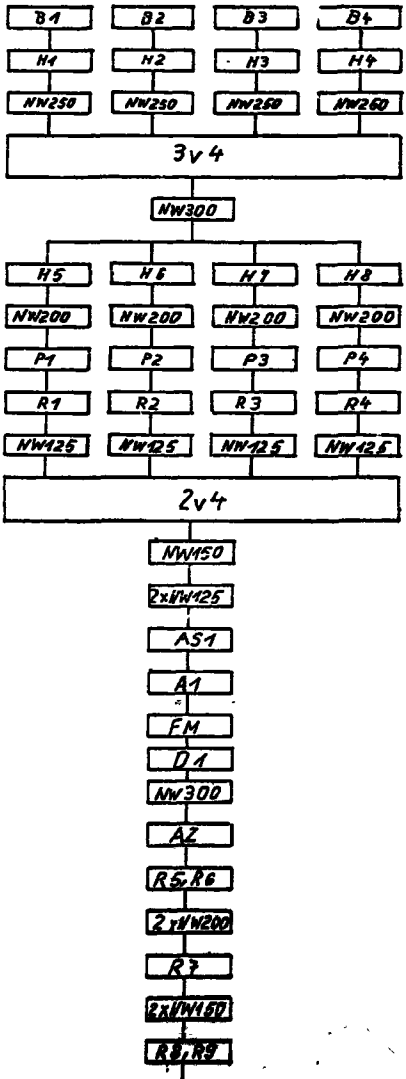


Fig. 4 Flow-Diagram of the Core-Flooding System for BWR

Reliability Diagram



Detailled Flow Diagram

Failure Rate 10^{-6}/h

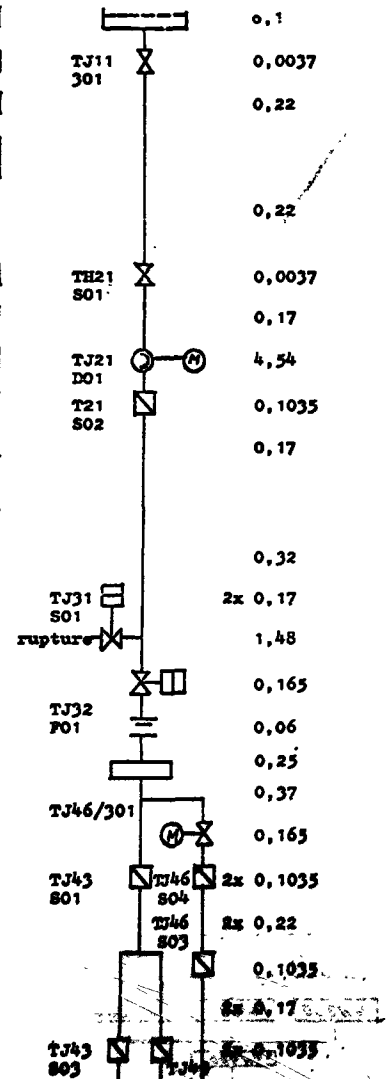


Fig. 5 High-Pressure-Water-Injection System

Detailled Flow Scheme
refueling water tanks

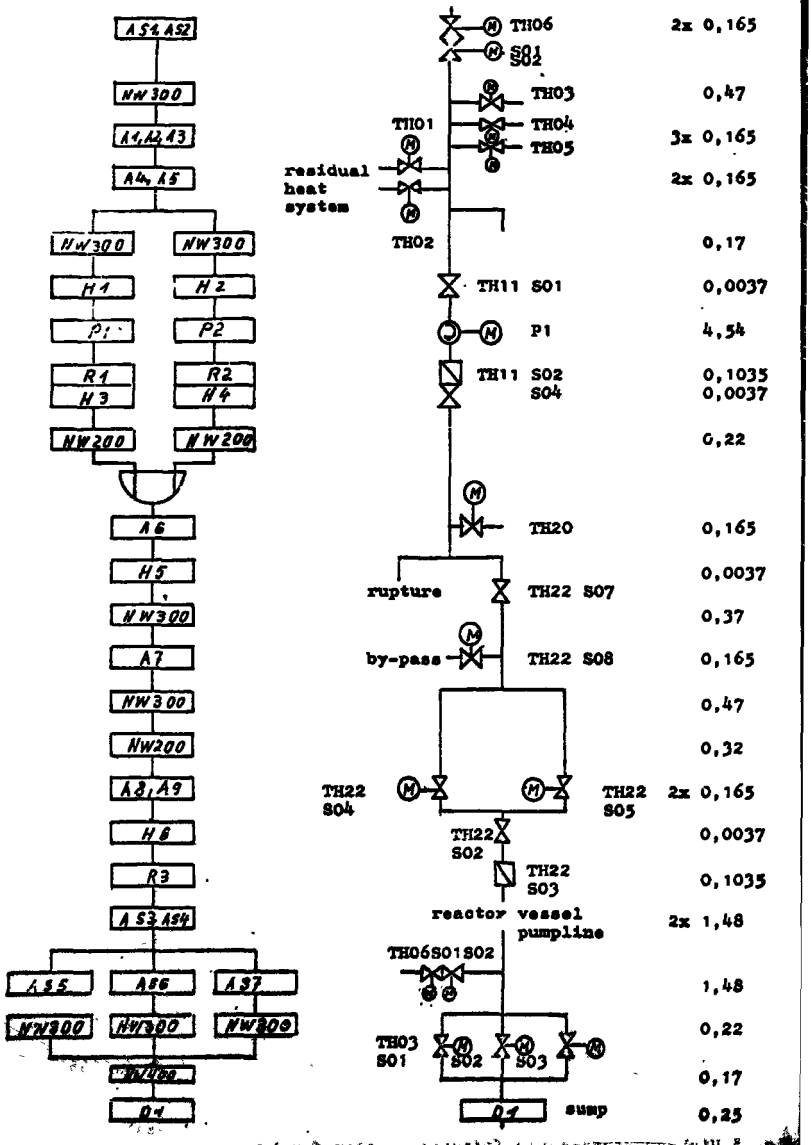


Fig. 6 Lay-out presented for discussion - Option for PWR

17 093/ 11/-

Reliability Diagram | Detailled Flow Scheme | Failure Rate 10^{-6}/h.

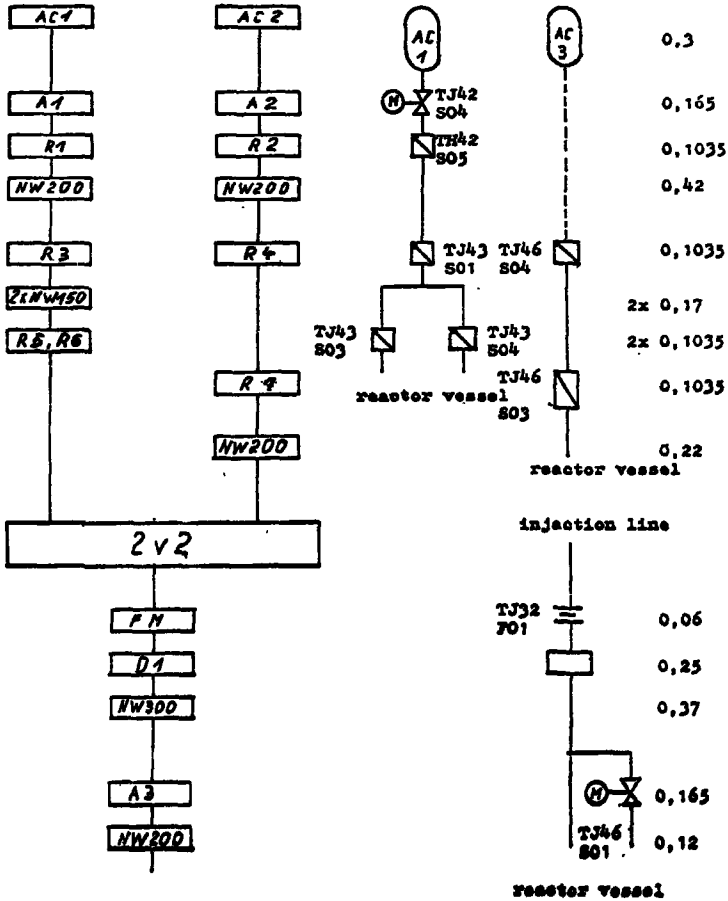


Fig. 7 Accumulator-System including connection Low-Pressure-Water-Injection-System (LPIS)

Reliability Diagram	Detailled Flow Scheme	Failure Rate $10^{-6}/h$
S1 S2 S3 S4 S5 S6		0,46
M1 M2 M3 M4 M5 M6		0,184
3 v 6		

S relief pressure valve
M solenoid valve

Fig. 8 Depressurisation-System for BWR

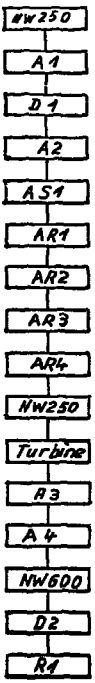
Reliability Diagram

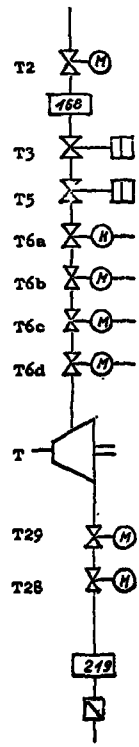
Detailled Flow-Schemo

Failure

reactor vessel

$\lambda \cdot 10^{-6}$/h





	0,25
T2	0,165
	0,25
T3	0,165
T5	1,48
T6a	0,282
T6b	0,282
T6c	0,282
T6d	0,282
	0,77
T	1,0
	0,165
T29	0,165
T28	0,37
	0,25
	0,1035

suppression pool

Fig. 9 High-Pressure-Water-Injection-System for BWR (1)

Reliability Diagram	Detailled Flow-Scheme	Failure Rate
	suppression pool	$\lambda 10^{-6}/h$

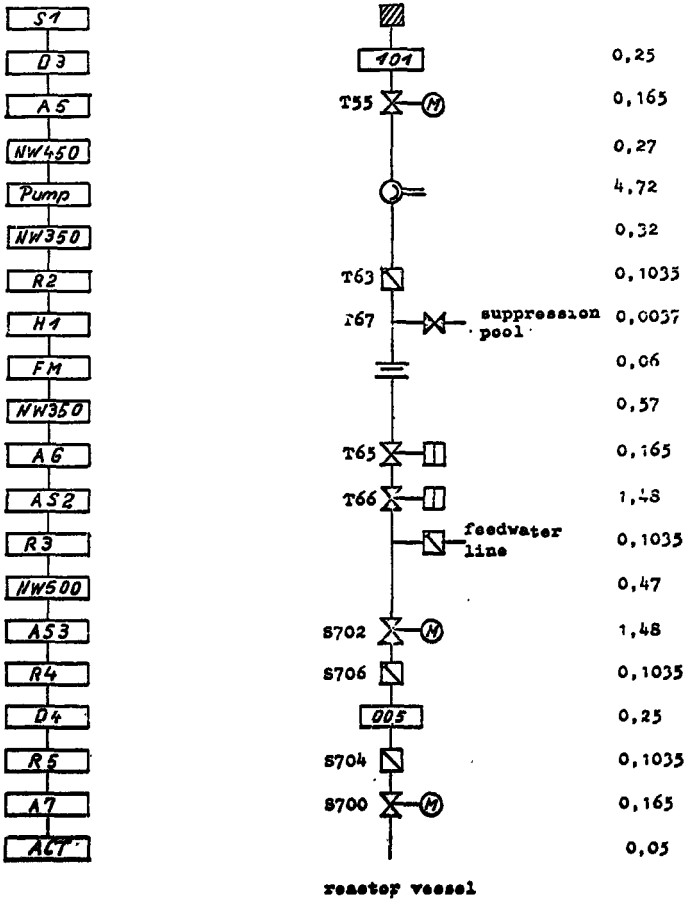
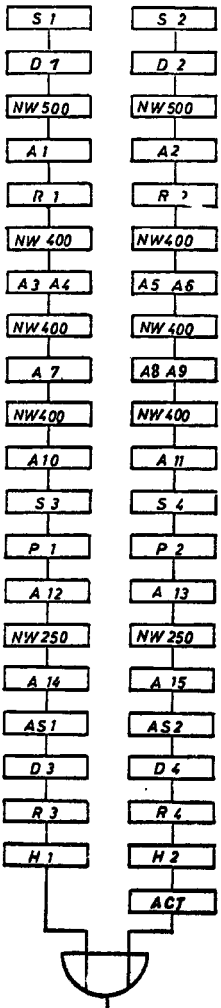


Fig. 9 High-Pressure-Water-Injection-System for BWR (2) (continued)

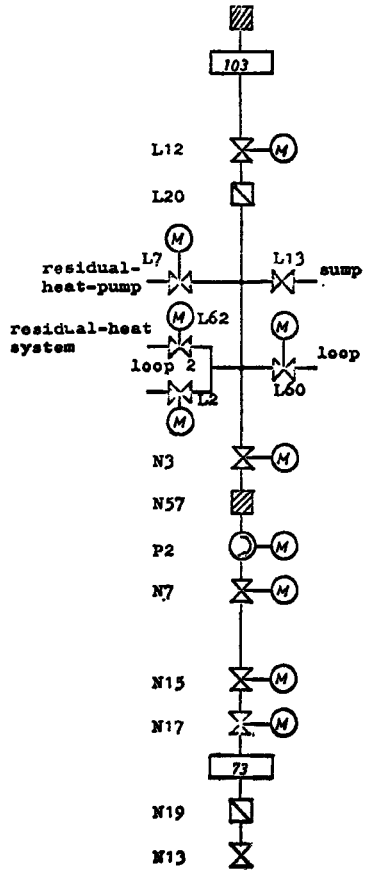
Reliability Diagram

Loop 1 Loop 2



Detailed Flow Scheme

Loop 2
suppression pool



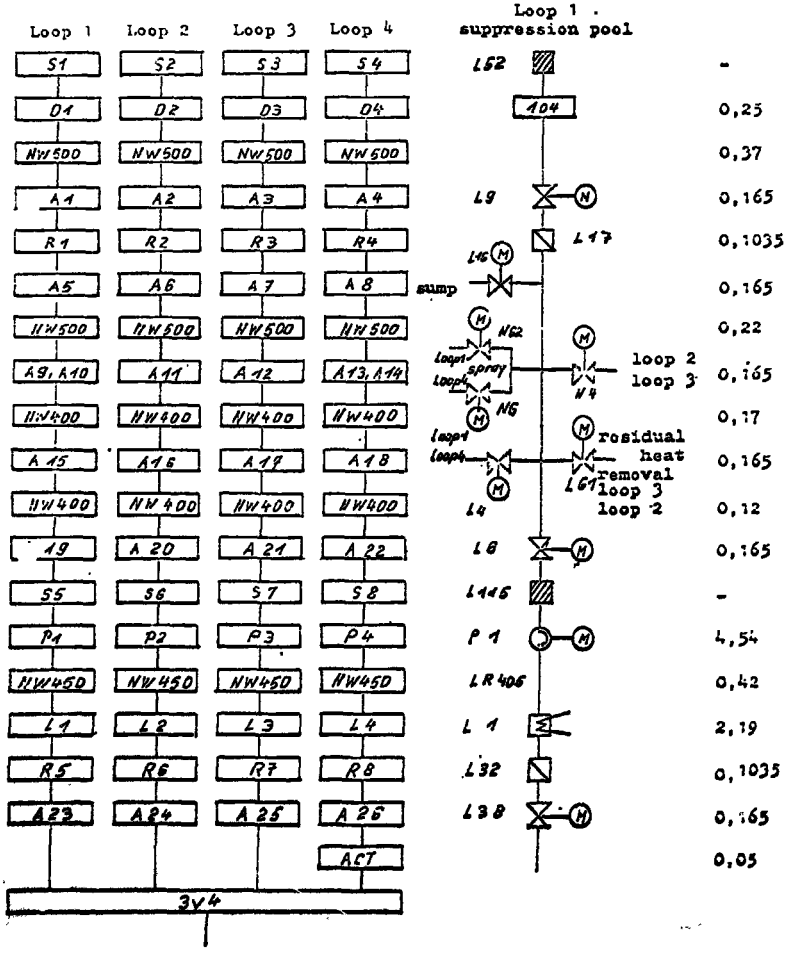
Failure rate

$\lambda 10^{-6}/h$

	—
	0,25
	0,37
	0,165
	0,1035
	0,22
	0,165
	0,22
	0,165(loop1
	2x 0,165(loop2
	0,27
	0,165
	-
	4,54
	0,165
	0,62
	0,165
	1,48
	0,25
	0,1035
	0,0037
	0,05

Fig. 10 Core-Spray-System Test [illegible]

Reliability Diagram | Detailled Flow Scheme | Failure Rate $10^{-6}/h$



Core-Flooding-System for BWR (1)

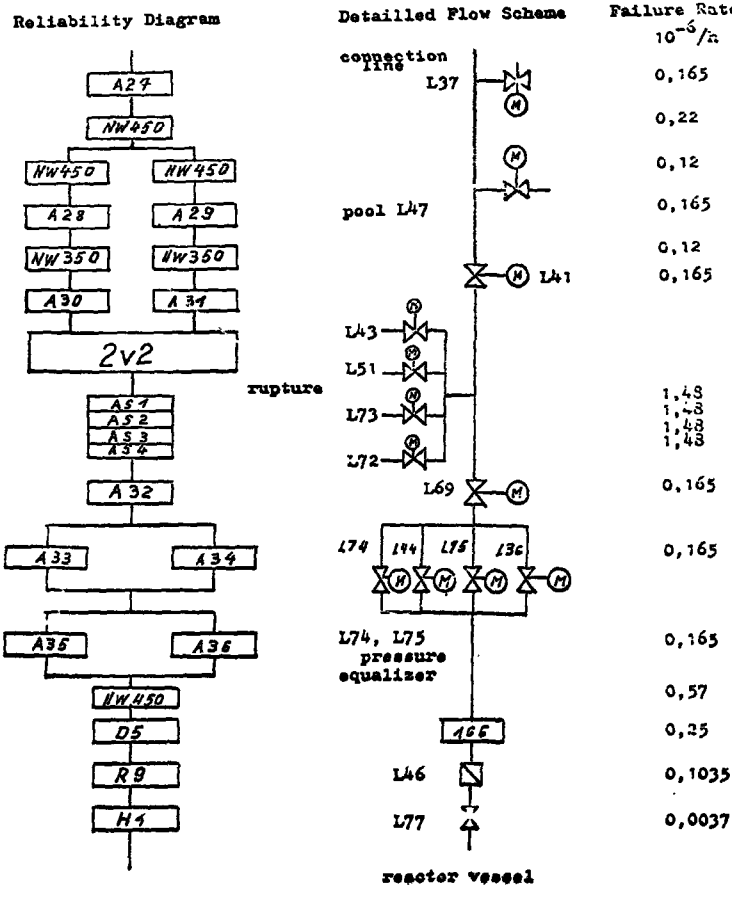
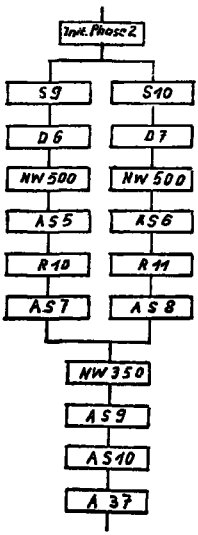
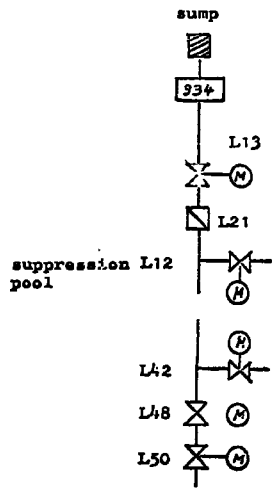


Fig. 11 Core-Flooding-System for BWR (8)

Reliability Diagram



Detailled Flow Scheme

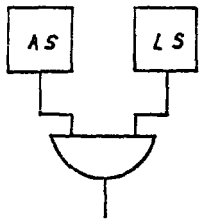


Failure Rate $10^{-6}/h$

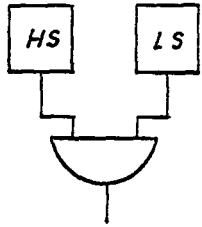
sump	-
934	0,85
L13	0,37
	1,48
L21	0,1035
suppression pool L12	1,48
	0,27
L42	1,48
L48	1,48
L50	1,65

Fig. 11 Core-Flooding -System for BWR (3)

1. Rupture of the Main Coolant Line



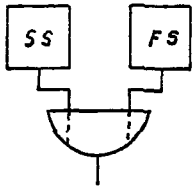
2. Rupture of the Pressurizer Line



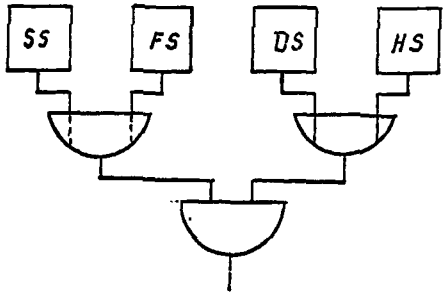
HS High-Pressure-Water-Injection-System
LS Low-Pressure-Water-Injection-System
AS Accumulator-System

Fig. 12 Total Reliability Diagram of the ECS for PWR

1. Rupture of the Main Coolant Line



2. Rupture of the Injection Line



SS Core-Spray-System
FS Core-Flooding-System
DS Depressurization-System
HS High-Pressure-Water-Injection-System

Fig. 13 Total Reliability Diagram of the ECS for BWR

ONTARIO HYDRO
NUCLEAR GENERATING STATION
SAFETY AND PRODUCTION RELIABILITY

R.J. Kelly

Ontario Hydro

Toronto, Canada

Presented to the Meeting of Specialists on the Reliability of Mechanical Components and Systems for Nuclear Reactor Safety. Organized by the Committee on Reactor Safety Technology of the European Nuclear Energy Agency and held at Risø, Denmark, September 24 - 26, 1969.

SUMMARY

Ontario Hydro's present nuclear power program involves four nuclear-electric generating stations, two of which are now in operation while the remaining two are under construction.

Several years ago in Canada, nuclear safety standards were defined in mathematical terms as guides for determining the required reliability of nuclear safety systems. Experience from our operating stations has led to the development of techniques to measure and compare component performance with these safety standards and similar techniques are now being developed to define electricity production targets and compare equipment performance with these.

This paper traces the development of both the safety and production reliability standards, reviews experience with various equipment at the operating stations in terms of these standards and describes how this experience is being applied to the stations now under construction.

C O N T E N T S

0. INTRODUCTION

Ontario Hydro is a publicly-owned electric utility with a dependable peak capacity in excess of 10,000 MW(e) at the end of 1968. The committed nuclear program involves four nuclear power stations all equipped with heavy water moderated and cooled, natural uranium (*CANDU*) reactors. Two of these stations are presently in operation while the remaining two are under construction. The single unit 22 MW(e) NPD was placed in service in 1962 (1) and the single unit 208 MW(e) Douglas Point Generating Station was placed in service in 1968 (2). The first of four 508 MW(e) units of the Pickering Generating Station is scheduled for operation in 1971 while the first of four 750 MW(e) units of the Bruce Generating Station is scheduled to begin operation in 1975.

Reliability studies for these stations focus on two main areas, safety and production. Safety reliability studies are directed towards ensuring that risks of dangerous equipment failure are acceptably low. At the same time production reliability is of major economic concern and studies in this area are directed towards equipment improvements which will reduce lost production. Although the goals are different similar techniques are used for both types of study in Ontario Hydro to set up information collection systems and to develop component standards for judging component performance.

The intent of this paper is:

(1) To describe the safety and production reliability standards which have been adopted and to describe techniques used to gather equipment fault data to enable equipment performance to be compared to these standards.

(2) To review experience with reactor regulating and protective systems for comparison with the standards.

(3) To review experience with particular mechanical systems at the nuclear stations such as emergency cooling systems, fuelling machines and standby generators and to compare this experience to the safety and production reliability standards.

1. RELIABILITY STANDARDS AND ASSESSMENT

There are two basic reasons for striving for a high standard of equipment reliability at nuclear stations. The first is to ensure that the risks of dangerous equipment failure are low enough to provide an acceptable safety standard. The second is to ensure that the risks of equipment failure leading to a loss of electricity production are economically acceptable.

For these reasons we have developed for Ontario Hydro nuclear power stations two separate standards to use as targets for equipment performance, a nuclear safety reliability target and a production reliability target. Performance of all equipment at our nuclear power stations is measured against these targets.

1.1 NUCLEAR SAFETY RELIABILITY

In the early stages of reactor development extensive safety measures were often applied without much knowledge of their effectiveness or reliability or of the magnitude or probability of the disaster they were intended to avoid. These measures added considerably to cost and plant complexity and the net increase in safety was obscure.

In Canada (3) the search for a nuclear safety standard led to an initial philosophy of defining as an acceptable public risk from a nuclear establishment one which was equivalent to that associated with other enterprises of equal economic worth. Many safety factors were applied to offset unknowns associated with the nuclear stations, however, the result was that the maximum acceptable nuclear accident risk for stations such as NPD and Douglas Point was described as being in the range of 10^{-5} to 10^{-6} per year.

This type of standard was used to judge the adequacy of the design of these stations, however, the number is so small that it is obviously impossible to provide any single system or piece of equipment with adequate reliability to meet the standard. The approach which has been used is to arrange the plant so that no nuclear accident can

occur unless there are simultaneous failures of several pieces of independent equipment. This sharing of the reliability requirement results in equipment failure rate targets which could be met realistically by the designer and which can be demonstrated in a relatively short time by operating experience.

This philosophy has been further refined in recent years and has led to the preparation of a Siting and Design Guide by the Atomic Energy Control Board which is the federal government agency responsible for licensing nuclear stations in Canada (4). The basic assumption of this Guide is that nuclear plant is separated into three groups for purposes of safety evaluation. These groups are:

1. The process equipment which includes all the equipment and systems necessary for the normal functioning of the reactor and generating unit.

2. The protective equipment which includes all the systems or devices designed to prevent damage to the fuel resulting from any failure of process equipment.

3. The containment provisions which includes any structures or other provisions which are intended to restrict or limit the release of any radioactive materials that might escape from process equipment.

A fundamental principle of this approach is that these three groups of equipment are structurally and operationally independent to the extent that the probability of a cross-linked fault, that is, one affecting equipment in more than one group, is small compared to the coincidence of independent faults. Thus, for analysis purposes, the probability of simultaneous equipment failure is calculated as the product of the individual equipment failure probabilities.

The standards of equipment reliability are similar to those developed previously for setting a permissible accident risk of 10^{-5} to 10^{-6} per year. They are:

1. Single Failures - failures of process equipment which could lead to a dangerous release of radioactivity, but are safely terminated by operation of protective and containment equipment, should not exceed 1/3 per year.

2. Dual Failures - failures of process equipment potentially leading to a dangerous release of radioactivity, combined with a coincident failure of either the protective or containment equipment, should not exceed an annual risk of 10^{-3}.

A common characteristic of the protective equipment and containment provisions, or the safety systems as they are commonly called, is that the systems are normally idle and failures which may defeat the system remain hidden until revealed by a test or other call for operation. In Canada, we use the term unreliability to describe the portion of total time that a safety system would be expected to fail if called upon to operate. For most equipment, failure rates are independent of test frequency so that unreliability can be reduced by increasing test frequency. As an example, increasing the test frequency by a factor of 2 reduces the unreliability by the same factor for a fixed equipment failure rate and we use this technique to adjust equipment unreliability.

The probability of a dual failure, as considered in the Siting Guide, is calculated as the product of the process equipment failure rate and the protective equipment unreliability.

At our nuclear stations we set a permitted unreliability standard for each safety system then establish a fair share of this system total for the various subsystems and components. Table 1 indicates the application of this technique to the Boiler Room Area Containment system at NPD. This system is made up of three major subsystems, one for providing initial pressure relief of the area, one for isolating the area and one for limiting pressure within the isolated area by dousing.

In this example the maximum permitted unreliability of the total system is fixed at 10^{-2}, however, the portion assigned to the various subsystems and components is flexible. Poor performance on the part of one group of components can be offset by better than expected performance by another group and extensive use is made of the capability of test frequency increases to reduce component unreliability.

1.2 PRODUCTION RELIABILITY

For our applications we consider production reliability to be the ability of a generating unit to deliver electricity when required. This is a general term and we have developed several other terms to simplify our calculations of production reliability.

1. Capability refers to the ability to produce electricity using an energy basis and thus provides a comparison between the actual energy production and the maximum possible energy production.

   Availability refers to the ability to produce electricity using a time basis and thus it is a measure of the time during which the unit is able to produce power.

2. For simplicity of calculation we normally use the complimentary terms incapability and unavailability as a measure of the inability of the unit to produce electricity.

3. Incapability may result from a unit being shut down (outage) or reduced to part load (derating) and these outages and deratings in turn may have been planned for ahead of time (planned) or they may be the result of unexpected conditions (forced).

4. The net output of a unit is the net energy in MWh delivered to the transmission system for a specified time. The entire time interval is considered including the period when the unit is shut down or derated.

   The net capacity factor is the ratio of the actual net output to the net output a unit could deliver if it operated perfectly at full capacity for the entire time interval.

Nuclear generating units in the Ontario Hydro system will be operated as base load units and an average lifetime net capacity factor of 80 percent is assumed for the Pickering units. In our analysis we assume that the availability of nuclear units will be similar to that of equivalent fossil units and that availability will be lower during the early life or immaturity period. This is reflected in the predicted capacity factor variation shown for Pickering GS in Table 2.

We also expect that availability will decrease with unit size and this is illustrated by comparing the Pickering incapability targets with those which have been set for NPD and Douglas Point as follows:

NPD	- 1.7% (Forced Outage and Derating), 3.4% (Total)
Douglas Point	- 2.7% (Forced Outage and Derating), 7.2% (Total)
Pickering	- 5.2% (Forced Outage and Derating), 10.0% (Total)

Shutdown preventative maintenance normally is done during planned shutdown periods while emergency maintenance is carried out during forced shutdown or derating periods. The total incapability target for a nuclear generating unit includes incapability caused by both planned and forced outage and derating.

Since it is a demonstration station, NPD is frequently shutdown for experiments, training and tests thus providing an additional opportunity for planned maintenance. During the winter months no shutdowns are planned so that total incapability during this period is equal to the forced outage and derating incapability and the target net capacity factor is based on this. Tables 3 and 4 compare the achieved net capacity factor to our targets since 1962.

Just as a system was developed for sharing safety system unreliability targets among the various sub-systems and components so we have developed a system for sharing unit incapability targets among the various plant systems. To establish the relative fair share for each system we felt it was necessary to recognize two basic parameters. These were; first, the complexity and worth of equipment as indicated by cost and second, the likelihood of the equipment failure causing unit outage or derating.

The system we have adopted involves distributing the unit incapability target in proportion to the total cost of each system modified by a Relative Proneness Factor (RPF). The RPF mainly identifies whether a system can cause a loss of production or not and to date we have restricted our analysis to three degrees of RPF.

RPF = 0	for systems whose probability of causing an outage is zero
RPF = 0.1	for Buildings and Structures which could conceivably cause an outage
RPF = 1.0	for all mechanical, electrical and instrument systems which are likely to cause or contribute to an outage or derating should they fail.

The incapability allocation for the various NPD systems is summarized in Table 5.

Information of this type provides a guide for the system designer to judge relationships between equipment performance and economic requirements and it provides the operator with a tool for measuring equipment performance.

1.3 RELIABILITY MEASUREMENT

1.3.1 Data Collection

A single form (Figure 1) is used at all Ontario Hydro nuclear power stations for reporting all component faults. This multi-copy form, which is identified as a Deficiency Report, serves two main purposes:

1. The form provides a method for reporting all faults and deficiencies to the responsible work unit and thus serves as a work order.

2. Analysis and corrective action taken by the work unit are recorded on the form which is placed on the equipment file so that the form provides a complete fault record.

Since the single form is used to record all types of faults, a review of the Deficiency Report file for a particular system or piece of equipment will indicate all faults which affect both the safety and production reliability targets for the equipment.

Two other types of forms are used to provide data required for reliability analysis.

All safety systems are tested at regular intervals as calculated from unreliability targets. For each type of test, forms have been prepared specifying such detail as test procedure, expected component response, etc. These forms are forwarded to the tester at scheduled dates and completed forms placed in the System Test file. Since the forms are designed for each type of test we have not developed any standard test form style.

Each time a unit outage or derating occurs an outage report is prepared. These forms contain such detail as the outage or derating duration, system or equipment causing the outage and system or equipment prolonging the outage. A sample of the type of form used is shown in Figure 2.

1.3.2 Reliability Analysis

Several times per year at each nuclear station a complete review is made of the performance of all process, protective and containment equipment which affects the nuclear safety standard. This review requires an examination of all related Deficiency Reports and classification of the various faults. In

addition, the test records of the protective and containment equipment are reviewed and calculations made of system and component unreliability for comparison with targets. Finally, arrangements are made for test frequency adjustment or component modification to bring expected unreliabilities in line with the targets.

To date production reliability reviews have been carried out less frequently than the safety reviews. The production reliability review starts with an examination of the various outage reports and calculation of the total unit incapability and the incapabilities chargeable to the various systems. When a system has been identified as having exceeded the incapability target, the Deficiency Reports are examined to pinpoint actual component faults.

At the present time we are actively investigating the use of computers for fault data storage and analyses. One current study, associated with the Douglas Point GS reactor regulating and protective systems, involves the preparation of a computer program which will receive information on component behavior, recognize and classify faults and calculate component and system unreliabilities. If the study indicates that this type of computer application is successful we will extend it to cover other station systems and also provide production reliability information.

2. REGULATING AND PROTECTIVE SYSTEM RELIABILITY

2.1 SYSTEM DESCRIPTION

The reactor system design of all Ontario Hydro nuclear generating units follows the same basic concept characterized by a horizontal pressure tube reactor, heavy water moderator and heat transport (coolant), natural uranium oxide fuel and on power refuelling. The basic flow diagram is shown in Figure 3.

The heat generated in the fuel is transferred by the heat transport fluid to the steam generator. The steam generator consists of one or more heat exchangers and steam drums in which steam is generated from ordinary water. The steam thus produced is used to drive the turbine generator. The quantity of steam admitted to the turbine is controlled by a set of steam throttle valves. After passing through the turbine the low pressure, low temperature steam is condensed by cooling water and returned to the steam generator through a conventional feedheating system.

The reactor consists of a tank and tube assembly called a calandria which holds the heavy water moderator. The fuel and heat transport heavy water are contained in zirconium alloy pressure tubes which pass through the calandria tubes and are centred in them by spacers. Each end of the pressure tube is fixed in an end fitting to which the fuelling machines are attached for fuel changes.

Reactor power regulation is achieved by variation of moderator level, insertion of absorber or booster rods or addition or removal of dissolved poison. The NPD reactor normally uses only moderator level control while the Douglas Point and Pickering reactors employ all three methods.

In the NPD system vacuum pumps reduce the pressure over the upper surface of the moderator in the calandria below the pressure in the dump tank. Fine control of the pressure differential, and hence moderator level and reactor power, is provided by varying the opening size of the regulating valves which bypass the vacuum pumps.

To trip or scram the reactor in the event a critical variable exceeds a prescribed limit, the differential pressure is reduced to zero by the rapid opening of dump valves which causes the moderator to drop into the dump tank.

The reactor protective system, which controls dump valve position, is triplicated. The six dump valves are arranged with two valves in series in each of three parallel pipes so that opening of both valves in any one pipe destroys the pressure differential causing a reactor trip. Each of the three protective channels controls one valve in each of two pipes, thus opening of any two of three channels will cause a reactor trip. At the same time any one of the protective channels can be removed from service and its dump valves opened for test while the reactor remains at high power.

The reactor regulating system is a similar but completely independent system which is also triplicated and which controls reactor power by controlling regulating valve position. The six regulating valves are arranged similar to the dump valves.

The regulating and protective systems receive independent information from independent detectors on important variables, such as neutron power, heat transport pressure and temperature, moderator level, etc.

At Douglas Point the main change involves the use of control rods for minor adjustment of reactor power so that the calandria normally remains full during operation.

At Pickering, shutdown rods have been provided. These are normally dropped on a signal for reactor trip so that the dump system remains as a backup and will not operate unless a reactivity reduction fails to proceed at a predetermined rate. This allows a rapid restart following a transient trip by avoiding delays associated with calandria pump up.

2.2 RELIABILITY EXPERIENCE

Our most complete experience to date with regulating and protective systems has been provided by NPD, which has been in operation since 1962, and for this reason our reliability analyses have focussed on results from this station.

2.2.1 Nuclear Safety Reliability

In our system for deriving nuclear safety standards, regulating systems are classed as process equipment, which by definition has a permissible annual unsafe failure rate of approximately 1/3, while protective systems fall in the category of protective equipment which allows a permissible unreliability, or portion of total time in a failed condition, of between 10^{-2} and 10^{-3}. For the NPD systems, which represented our initial efforts to meet these standards, we felt that additional safety factors were desirable, thus we set as our targets a maximum annual regulating system unsafe failure rate of 10^{-2} and a maximum protective system unreliability of 10^{-4}.

To meet these high standards a program of daily tests of each regulating and protective system channel was instituted in 1962. These tests mainly involve injecting a synthetic signal in a single channel and observing that instruments and valves respond correctly. Detailed reviews are made periodically of all test sheets and fault records to produce safety reliability statistics.

In our reliability analyses we review both cross-linked faults which affect more than one set of instruments or channel and single component faults. We have had very few cross-linked faults and have never had an unsafe failure which resulted in the regulating system demanding an unsafe power increase or the protective system failing to shut down the reactor when required. Thus, our calculations of regulating and protective system reliability mainly involve deriving the probability of

unsafe system failure through the application of standard probability calculations to our experienced individual component failure rates. Our reviews to date indicate that the unsafe failure rate of the regulating system remains below our target of 10^{-2} per year and the unreliability of the protective system has consistently been several orders of magnitude below the maximum target unreliability of 10^{-4}. As a result of this experience with the protective system, we have reduced our test frequency from once per day to twice per week.

The regulating and protective systems at NPD have not been without component faults, as indicated in Table 6. Many of these faults were associated with mechanical devices, such as retransmitting slide-wires, balancing motors, etc., which employ moving parts to transmit information. In recent years reliable solid state devices have been perfected and this type of component is being used in the Douglas Point and Pickering stations.

2.2.2 Production Reliability

As a small demonstration station, NPD is used for training and equipment testing as well as electrical production, thus the periods of sustained production are usually limited to predetermined demonstration runs. It is during these runs that attempts are made to eliminate outages and unit derating and compare actual unit and system incapability with the targets.

The performance of the NPD unit during eleven demonstration runs is shown in Table 4.

Between 1964 and 1966 there was a total of 119 outages of the NPD unit, of which 29 were for training, 21 were planned or maintenance outages and 69 were forced outages. During the same period there were 31 reactor trips from high power, seven of which were deliberately planned for training.

During the period between 1964 and 1966 six of the forced outages were charged against the regulating system, while eight of the forced outages were charged against the protective system. During this period the incapabilities of both the regulating and protective systems were considerably above the maximum targets; however, since that time the incapabilities of both systems have been brought down to approximately target level, as indicated in Table 7.

3. RELIABILITY OF MECHANICAL SYSTEMS

Some mechanical systems are provided as a safety measure and they may have little effect on the production of electricity, other systems play a major part in production but have a minor effect on nuclear safety. All mechanical systems in Ontario Hydro nuclear stations are measured against both the nuclear safety and production reliability standards. As a result one of the standards for a particular system may prove to be a difficult target to meet while the other standard can be met very simply and only periodic checks are required to ensure conditions have not changed.

Experience with three different systems is described in this section. These systems have been selected to show the variation in targets chosen for different systems and some of the efforts we have made to meet these targets.

1. Fuelling machines - Nuclear generating units in the Ontario Hydro system are designed for on-power fuel replacement, and these machines are frequently in operation while the unit is producing. Fuelling machine breakdown may result in unit shutdown or derating and so the machines have a significant effect on production reliability. On the other hand, the machines are designed for fail safe operation and they have not presented any significant problems in meeting nuclear safety standards.

2. Standby generators - these are protective devices which are normally idle when the unit is producing. They have a moderate effect on the nuclear safety standard and a minor effect on production reliability. The standby generators are sometimes operated to provide additional generation during extreme system peak conditions, thus introducing a further economic consideration towards their reliability.

3. Emergency cooling systems - these are classed as protective equipment, or safety systems, and they are normally idle when the unit is producing. These systems have a relatively minor effect on the production standard but they are of vital importance to the safety standard and considerable effort is required to ensure that they meet their share of this standard.

3.1 FUELLING MACHINE RELIABILITY

3.1.1 General Description

The basic design of the Canadian on power fuelling system has been described by McConnell (5) and the major features of this concept are illustrated in Figures 3,4,5 for NPD. The major features of the Douglas Point and Pickering fuelling machines are similar, although there is some variation in equipment orientation.

To change fuel "on power" two machines each clamp onto an end fitting associated with a selected fuel channel. Seal plugs are removed at each end and one machine pushes a new fuel bundle into the channel while the other machine receives a spent fuel bundle. The seal plugs are then replaced, the fuelling machines unclamp from the end fittings and the spent fuel is discharged to a spent fuel bay. All operations are directed remotely from the control room.

3.1.2 Reliability Experience

In the Canadian system of classifying station systems for nuclear safety standards, the fuelling machines come in the category of process equipment. For this type of equipment our standard specifies that the rate of dangerous faults should not exceed 1/3 per year and we have only had one fault which could fit this category.

During commissioning of the NPD fuelling machines in 1962 while attemping on power fuelling for the first time one machine was not tightly clamped onto the end fitting when the seal plug was removed. As a result, a gap existed between the end fitting and the fuelling machine which allowed some escape of heat transport water from the fuel channel into the reactor vault. The subsequent drop in heat transport pressure caused an immediate reactor trip while the entry of hot water into the reactor vault initiated operation of a dousing system to limit pressure in the room. All protective and containment equipment operated as designed to safely terminate the incident.

Changes were made to eliminate this type of occurrence and the NPD fuelling machines have been performing on power refuelling routinely since January 1, 1964.

During the three year period between 1964 and 1966 the average incapability for the NPD unit was 11.6% compared to an annual target of 4%. The production reliability review indicated that 97% of the lost production was due to 10 systems and of these the fuelling system contributed the largest share.

This focussed attention on the need to improve fuelling machine reliability and the rapid improvement in performance of these machines is demonstrated by the following statistics.

NPD FUELLING SYSTEM INCAPABILITY EXPERIENCE

	Incapability Target	Actual Incapability		
		Outage	Derating	Total
	%	%	%	%
1964	0.65	2.86	0.32	3.18
1965	0.65	6.76	2.17	8.93
1966	0.65	0.83	0.34	1.17
1967	0.32	0	0	0
1968	0.32	0	0	0

This dramatic improvement was not entirely a result of better fuelling machine performance singe NPD was shutdown for several months in 1968 while the heat transport was changed from a pressurized heavy water to a boiling heavy water system.

3.2 STANDBY GENERATOR RELIABILITY

3.2.1 General Description

The arrangement of electrical power supplies at Canadian nuclear power stations was reported by Hake (6).

As indicated in Figure 6, station service power consists of either three or four "classes" of power, each with its own set of busses. These are listed in ascending order of reliability.

1. The Class IV busses are supplied from the generator and transmission lines through the station service transformers.

2. The Class III busses are normally supplied from Class IV but in emergency are supplied by standby generator units.

3. The Class II busses are supplied from Class III but in emergency service is sustained through motor generator sets operating on the station direct current supply.

4. Class I is the station direct current supply, normally fed through rectifiers or the motor generator sets and supplied, in emergencies, from the station batteries which float on this supply.

Equipment which is supplied from the Class III busses is generally of the type which can tolerate an outage of a few minutes without affecting the safety of the station. This includes such services as the firefighting pumps, moderator pumps and heat transport standby cooling pumps.

At NPD one 175 kva diesel-generator was originally supplied; however, a second 175 kva unit was installed in 1963 during the final stages of station commissioning. Both units are capable of supplying all essential Class III loads.

At Douglas Point two 950 kva diesel-generators were originally supplied and a third 1200 kva unit was added in 1969. Each diesel is capable of supplying all essential Class III loads.

At Pickering the Class III loads for each pair of 508 MW(e) nuclear generating units will be supplied from a set of 3 - 5000 kva combustion turbine generators. Each combustion turbine generator will supply all essential Class III loads for one nuclear generating unit.

3.2.2 Reliability Experience

The main safety requirement for standby generating units is that they, in conjunction with other sources of electrical power, maintain an electrical supply with a low enough unreliability that it does not significantly affect failure rates of essential process, protective or containment equipment. Our

analyses indicate that our safety standards will be met if diesel starting failure rates do not exceed 0.25 failures per test start.

Each diesel unit at NPD and Douglas Point is routinely test started once per week.

NPD experience has been favourable. During the four year span from 1965 through 1968 there was a total of 7 starting failures for the two units which represents a failure rate of less than 0.02 per unit per test.

Douglas Point experience has been much less favourable. Test data accumulated to the present time indicates a failure rate of 0.1 per unit per test. Although this performance meets our safety standard, it is well below the performance that has been experienced at NPD and other similar installations.

This poor diesel performance does not directly affect our production reliability standards since single diesel starting failures do not involve nuclear generating unit outage or derating. However, the diesel generating units are operated occasionally during extreme system peak conditions to provide additional generation capacity and this is one reason that we are attempting to bring the reliability of the Douglas Point units into the normal range experienced elsewhere.

3.3 EMERGENCY COOLING SYSTEM RELIABILITY

3.3.1 General Description

The major features of emergency cooling systems in Canadian nuclear power plants have been described by Brown (7) and the basic concept is shown in Figure 7. The common characteristic of all systems is that emergency injection is provided by feeding an alternate heat removal supply to the reactor using the existing heat transport inlet and outlet headers, feeder piping and fuel channels.

In the NPD design the light water dousing system storage tank is used as the alternate supply and this is connected by pipes directly to the heavy water heat transport system. The injection water is isolated by normally closed check valves and an air buffer space separates the heavy and light water to prevent downgrading when injection is not required. The system is designed to operate automatically when there is a sudden heat transport pressure drop as in a loss of coolant accident.

In later designs, as employed at Douglas Point and Pickering, the heavy water moderator is used as a source of injection water. This is normally separated from the heat transport system by closed isolating valves. Operation is initiated by instrument detection of low heat transport pressure which signals the motorized valves to open.

3.3.2 Reliability Experience

The NPD injection system has never operated nor has there been any occasions when operation was required. At various times the heat transport system has been depressurized for planned maintenance and care is required to ensure that before this is done the injection system is isolated by operation of manual valves. This procedure has not presented any problem.

There is no provision for testing NPD injection system components while the reactor is at high power and all components are tested semi-annually during a planned shutdown. There have been no unsafe failures of vital components and it is necessary that component failure rates remain very low in order that system unreliability targets will be met without an increase in tests to more than twice per year. No test frequency reduction is warranted in the near future, in spite of the very favourable test experience.

This is acceptable at a small demonstration station but we attempt to limit this type of shutdown test to once per year at the large nuclear units.

For the Douglas Point and Pickering design, provision has been made for testing vital components with the reactor at high power and this has enabled the safety unreliability target to be met with only once per year complete shutdown tests. This on power test capability also permits additional tests to be scheduled to compensate for higher than expected component failure rates without affecting production targets.

4. CONCLUDING COMMENTS

In developing numerical standards as targets for nuclear generating unit safety and production reliability, we recognize that some lack of reliability is inevitable and acceptable. Our studies show that similar techniques can be used to divide this lack of both safety and production reliability among the various systems and components. These techniques provide the designer with a tool for assessing relative cost and effort which should be employed to ensure the reliability of the system he is designing. At the same time, the techniques provide the operator with a tool for comparing experience with design goals and focus attention on equipment which is interfering most with unit performance.

We have been using these techniques for several years at NPD, and the lessons which we have learned are leading to modifications which will be applied at other nuclear power stations.

1. A capability for on-power testing of major safety system components is important This allows frequent tests to be done as dictated by the safety standard without unit shutdown or derating and resultant drop below the production standard.

2. Techniques used to share reliability targets among different systems and calculate unit targets by probability methods assume that the various systems and equipment are independent. At the same time there is an economic incentive to reduce capital cost by sharing services among various systems, thus, all common services must be arranged so that the risk of cross-linked faults is less than the risk of simultaneous independent faults.

3. Our methods for recording and correcting component faults have been successful at NPD, where the volume is small; however, we are preparing to have computer storage of fault data at the larger stations. We are also actively investigating the use of computers for analysis of fault data and reliability calculations.

REFERENCES

(1) NPD Operating Experience - E.P. Horton. Paper presented to the Symposium on Heavy Water Reactors, IAEA, Vienna 1967.

(2) Douglas Point Generating Station Commissioning - G.H. Williams. Paper presented to the Symposium on Heavy Water Reactors IAEA, Vienna 1967.

(3) Reactor Safety Practice and Experience in Canada - G.C. Lawrence, et al. Paper presented to 3rd UN Conference on Peaceful Uses of Atomic Energy, Geneva, September 1964.

(4) Containment and Siting Requirements in Canada - F.C. Boyd. Paper presented to the IAEA Symposium on Containment and Siting at Nuclear Power Plants, Vienna, April 1967.

(5) Canadian On-Power Fuelling Experience - L.G. McConnell. Paper presented to the American Nuclear Society Meeting, Denver, Colorado, June 1966.

(6) Field Experience in Canadian Nuclear Stations - G. Hake. Paper presented to the CREST Reliability Meeting, Ispra, Italy, June 1968.

(7) Emergency Cooling System in Canadian Nuclear Power Plants - W.S. Brown. Paper presented to the American Nuclear Society Meeting, Toronto, June 1968.

(8) Production Reliability of Nuclear Generating Units - K.E. Elston. Paper presented to the ANS/CNA Joint Conference, Toronto, June 1968.

(9) Some Control Features of Canadian Nuclear Generating Stations - K.E. Elston. Paper presented to the Eighth National Power Instrumentation Symposium, New York, May 1965.

TABLE 1

NPD Boiler Room Area Containment System
Expected System Unreliabilities - 1968

System	Subsystem	Component	Expected Unreliabilities		
			Component	Subsystem	System
Boiler Room Containment	Boiler Room Dousing	Dousing Valves	1×10^{-4}		
	"	Control Circuits	3×10^{-4}		
	"	Dousing Tank and Lines	1×10^{-3}	1.7×10^{-3}	
	Boiler Room Pressure Relief	Relief Diaphragm	4×10^{-4}		
	"	Exhaust Damper	2×10^{-3}		
	"	Control Circuits	6×10^{-4}	3.0×10^{-3}	
	Boiler Room Isolation	Relief Duct Gate	4×10^{-4}		
	"	Isolation Damper	3.5×10^{-3}		
	"	Control Circuits	(included above)	3.9×10^{-3}	8.6×10^{-3}

TABLE 2

Performance Targets - Pickering GS

Period	Year	Capacity Factor	Forced Outage and Derating Incapability	Total Incapability
		%	%	%
Immaturity	1	70	12	30
	2	75	10	25
	3	80	8	20
	4	85	6	15
* Maturity	5 - 30 (Excl. 2 Years)	82	5	10
Rehabilitation	2 Years	70	10	30
Lifetime Average		80	6	14

* During the maturity period production will be lost because of system conditions on occasions when the unit is capable of producing. The capacity factor is reduced by 8 percent in addition to the unit incapability to allow for this.

TABLE 3

Performance Targets - NPD 6S

Period	Year		Capacity Factor	Forced Outage and Derating Incapability
			%	%
Immaturity	1964 - 1965	Winter Peak	96	4
	1965 - 1966	"	96	4
	1966 - 1967	"	97	3
Maturity	1967 - 1968	"	98.3	1.7
* Immaturity	1968 - 1969	"	92	8

* Concept change from pressurized to boiling heavy water heat transport.

TABLE 4

NPD Capacity Runs

Run	Duration	Target Net Capacity Factor	Actual Net Capacity Factor
		%	%
1	Oct. 1 - Nov. 11/62	-	70
2	Feb. 12 - May 25/63	-	100
3	May 6 - Sept. 5/63	-	63
4	Dec. 18/63 - Apr. 17/64	85	88
5	Year 1964	80	82
6	Dec. 1/64 - Jan. 31/65	96	98
7	June 1/65 - June 30/65	90	75
8	Dec. 1/65 - Feb. 28/66	96	97
9	Dec. 1/66 - Feb. 28/67	97	98
10	Dec. 1/67 - Feb. 29/68	98.3	99.96
11	Dec. 1/68 - Feb. 28/69	92	86.8

TABLE 5

NPD G.S. INCAPABILITY TARGETS - MATURITY (TOTAL)

UNIFORM SUBJECT INDEX			INCAPABILITY %		
			OUTAGE	DERATING	TOTAL
0	GENERAL	Sub Total	.150	.020	.170
1	SITE AND IMPROVEMENTS	Sub Total	0	0	0
2	BUILDINGS, STRUCTURES AND SHIELDING	Sub Total	.077	.010	.087
	21 Powerhouse		.071	.009	.080
	22 Pumphouse		.003	.001	.004
	23 Stack		.001	.000	.001
	25 Outdoor & Underground Structures		.002	.000	.002
3	REACTOR BOILER AND AUXILIARIES	Sub Total	1.586	.210	1.796
	31 Reactor		.604	.082	.686
	32 Moderator System		.117	.015	.132
	33 Heat Transport System		.256	.034	.290
	34 Auxiliary Systems		.059	.008	.067
	35 Fuel Handling		.282	.038	.320
	36 Boiler Steam and Water		.012	.002	.014
	37 Fuel		.256	.034	.290
4	TURBINE GENERATOR AND AUXILIARIES	Sub Total	.244	.033	.277
	41 Turbo-generator unit		.206	.028	.234
	42 Main Condensing System		.005	.000	.005
	43 Feedwater		.014	.002	.016
	44 Reject System		.017	.002	.019
	45 Auxiliary Systems		.002	.000	.002
5	ELECTRIC POWER SYSTEMS	Sub Total	.154	.021	.175
	51 Output		.023	.003	.026
	52 Distribution		.100	.014	.114
	53 Lighting		.031	.004	.035

TABLE 5

UNIFORM SUBJECT INDEX			INCAPABILITY % OUTAGE	DERATING	TOTAL
6	INSTRUMENTATION AND CONTROL	Sub Total	.407	.054	.461
	60 General		.093	.012	.105
	63 Reactor Boiler and Auxiliaries		.229	.031	.260
	64 Turbine Generator and Auxiliaries		.014	.002	.016
	65 Electric Power Systems		.001	.000	.001
	66 Control Centre Equipment		.046	.006	.052
	67 Common Processes and Services		.024	.003	.027
7	COMMON PROCESSES AND SERVICES	Sub Total	.232	.032	.264
	71 Water Supplies		.098	.014	.112
	72 Sewage and Drainage		.016	.002	.018
	73 Ventilation		.094	.013	.107
	75 Compressed Gas Services		.024	.003	.027
	EXTERNAL	Sub Total	.150	.020	.170
	TOTAL		3.000	.400	3.400

TABLE 6

NPD Regulating and Protective System Faults

NPD Protective System

	1968	1967	1966	1965	1964	1963
Minor Faults	17	9	15	14	12	4
Safe Faults	16	15	3	17	15	22
Unsafe Faults	11	14	13	8	18	20
Total Faults	44	38	31	39	45	46

NPD Regulating System

	1968	1967	1966	1965	1964	1963
Minor Faults	41	24	34	28	68	34
Safe Faults	17	5	5	3	6	10
Unsafe Faults	9	0	10	12	15	20
Total Faults	67	29	49	43	89	64

TABLE 7

NPD Incapability Experience

NPD Regulating System

	Incapability	Actual Incapability		
	Target %	Outage %	Derating %	Total %
1964	0.05	0.17	0.27	0.44
1965	0.05	0.27	0.09	0.36
1966	0.05	0.01	0.05	0.06
1967	0.02	0	0.029	0.029
1968	0.02	0.076	0	0.076

NPD Protective System

	Incapability	Actual Incapability		
	Target %	Outage %	Derating %	Total %
1964	0.05	0.29	0.21	0.50
1965	0.05	0.78	0.25	1.03
1966	0.05	0.50	0.15	0.65
1967	0.02	0.016	0	0.016
1968	0.02	0	0	0

Originator Sends
Visits To Work Unit
Deliver To Planning Office
Book In Control Room

NPD G.S.
DEFICIENCY REPORT
WORK UNIT COPY

81188
REV. 11-62.

See - NPD G.S.
Stn. Instruction
No. 2.0.0.3.

To	SUBJECT	UBI.
ORIGINATOR STATES - Deficiency, Description, Symptoms, Circumstances, Etc.		SYSTEM
		DATE
		TIME
		FAILURE: SAFE / UNSAFE
		CATEGORY: MAJOR / MINOR
		SHUTDOWN REQ'D.: YES / NO
		ORIGINATOR
		SUPERVISOR
WORK UNIT STATES - Correction Description, Results, Comments, Etc.		DATE RECEIVED
		DATE COMPLETED
		WORK BY
		HOURS: REG. / O.T.
		DOSE MREM.
		PHOTOS
		ARCHIVE NO.
		DWG. CHANGE
		SUPERVISOR
OTHER COMMENTS		SHIFT SUPER. ASSEPT.
		INSPECTOR

FIGURE 1

IR 09002 _____

UNIT OUTAGE REPORT

OUTAGE NUMBER _____

OUTAGE TYPE ☐ FORCED ☐ MAINTENANCE ☐ PLANNED ☐ OTHER

OUTAGE CAUSED BY ☐ EQUIPMENT ☐ PERSONNEL ☐ CONDITIONS

INITIATED BY REACTOR TRIP YES NO

START	DATE	_____	HOUR	_____	MINUTE _____
FINISH	DATE	_____	HOUR	_____	MINUTE _____
DURATION	DAYS	_____	HOURS	_____	MINUTES _____

TIME ALLOCATION

FORCED	DAYS	_____	HOURS	_____	MINUTES _____
MAINTENANCE	DAYS	_____	HOURS	_____	MINUTES _____
PLANNED	DAYS	_____	HOURS	_____	MINUTES _____
OTHER	DAYS	_____	HOURS	_____	MINUTES _____

ENERGY LOSS ALLOCATION

USI	DESCRIPTION	TYPE	ENERGY LOSS
			Mw.h.
			Mw.h.
			Mw.h.
			Mw.h.
			Mw.h.
	XENON DERATING		Mw.h.
	TOTAL		Mw.h.

000-118 (R-5) FIGURE 2 Prepared by: _____

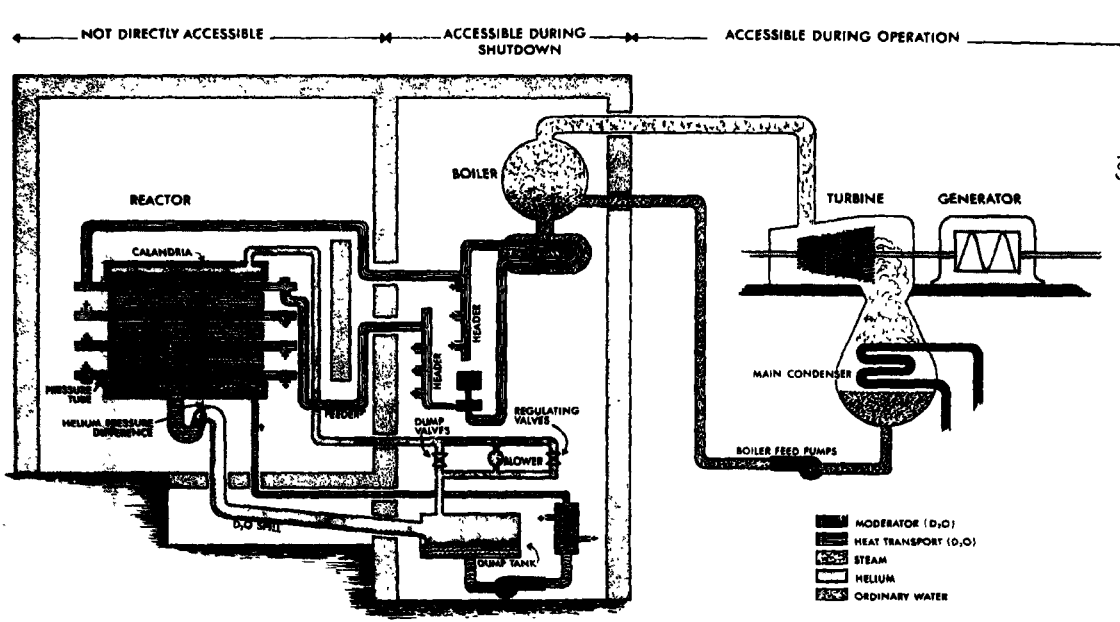


FIGURE 3

BASIC FLOW DIAGRAM

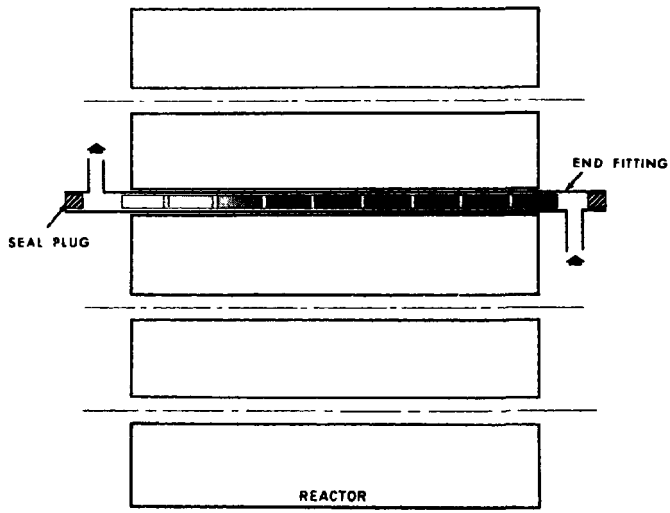


FIGURE 4

REACTOR FUEL CHANNEL ARRANGEMENT

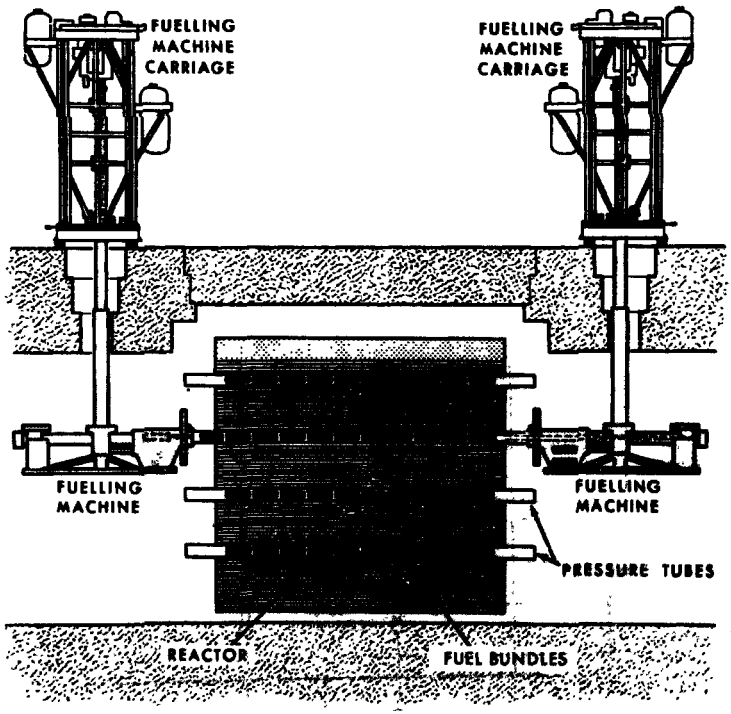


FIGURE 5

NPD ON POWER FUELLING

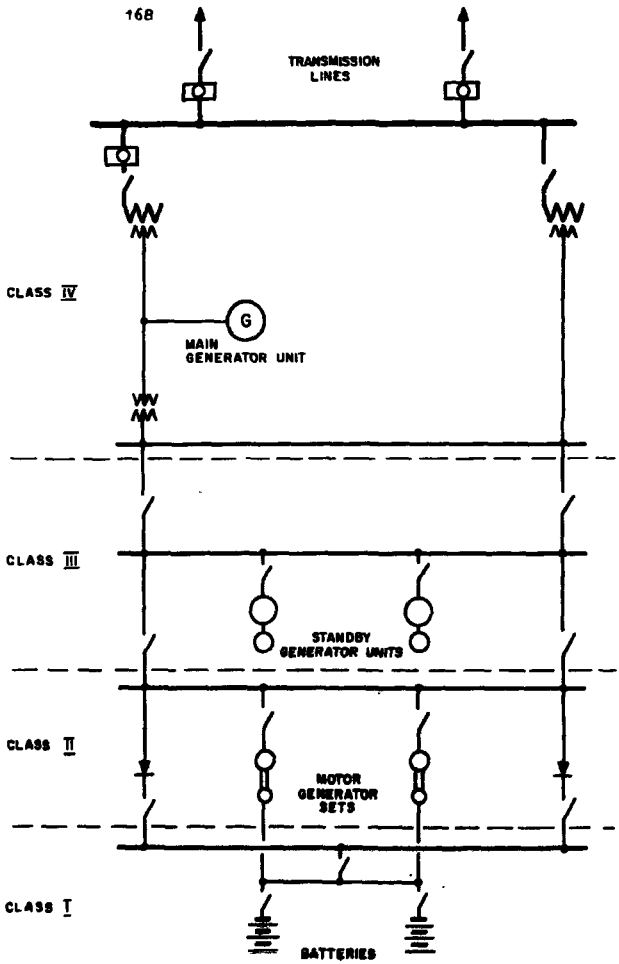


FIGURE 6

NUCLEAR UNIT ELECTRICAL SUPPLIES

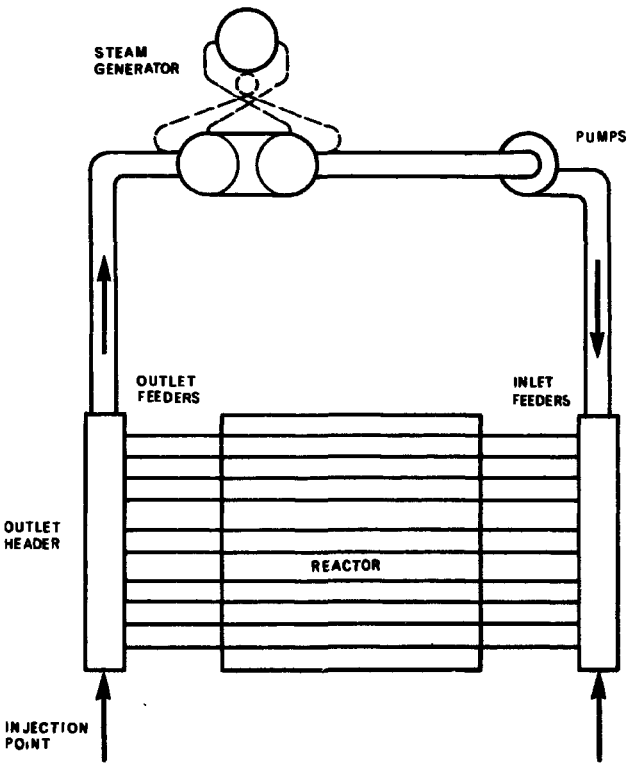


FIGURE 1

EMERGENCY COOLING INJECTION IN CANDU REACTORS

ENEA/CREST Meeting
Risø, 24th - 26th Sept. 1969

FREQUENCY AND CAUSES OF FAILURE TO COMPONENTS OF LARGE STEAM TURBINES

by

H. Huppmann

ALLIANZ Versicherungs-AG, München

Germany

For many decades now, the "Allianz Versicherungs-Aktiengesellschaft" has maintained a central card index for steam turbines of German ownership insured with its Machinery Insurance Department. To day, this card index contains approximately 1 700 turbines of all capacities up to 370 MW_{el} per turbo set of German manufacturers. Entered in this index are the most important failures as well as their causes. We have chosen for this conference a representative selection of modern turbo units ten years old at most, starting with a capacity of 100 MW. We considered 84 steam turbines, 51 of the reaction type and 33 of the action type, with a total capacity of 11 914 MW and a total of 3 481 000 hours of operation. The average unit load per steam turbine is 141,8 MW. The average number of hours of operation of each steam turbine is 41 440 hours.

We proceeded with the evaluation as follows: The number of the most important components was taken from production documents and from blueprints. The following components have been examined in detail: rotor blades of each stage, stator blades of each stage, nozzles and action wheels, journal and thrust bearings, cast-steel casings, rotors, labyrinth sealings and valves. If

we multiply the number of hours of operation of the different components with the number of components, we obtain for each turbo set and for each component, characteristic figures for reaction-type and action-type turbines. Thus, for example, the average reaction-type turbine achieves $4 \cdot 10^6$ ~~blade-hours~~ blade-hours of operation, whereas the action-type turbine achieves only $1.4 \cdot 10^6$ blade-hours. Similar figures were obtained for the other components. These values must be recalled to mind when considering the last two figures 10 and 11 in order to avoid too quick conclusions on the operational reliability of the entire system "steam turbine".

For example: The reaction-type turbine has on average a little less than three times as many blade-hours of operation per turbine than the action-type turbine. For this reason the action-type turbine can have about three times the probability of failure of the component "rotor blades" as the reaction-type turbine and still achieves the same reliability.

Let us begin to consider the graphs of the most important components of a steam turbine.

In Figure No. 1, we will show basically for all other following graphs what conclusions may be drawn from these evaluations. The horizontal axis shows the number of hours of operation from 0 to 41 400. This is the average number of hours of operation of all considered steam turbines. The vertical axis on the left shows the number of cases of failure, whereas the vertical axis on the right shows the frequency of failures in percentages. The straight-edged curve from 0 to 100 % shows the frequency of failures in the component "rotor blades". Immediately evident is the fact that 50 % of all failures already occur upto 8 750 hours of operation. The broken line from 0 to 100 % shows the linear distribution of failure. The variously cross-hatched bars on the horizontal axis represent the simple addition of failures in intervals of hours of operation.

Three basic types of failure-causes are clearly shown by three different types of cross-hatchings.

The first category is called "productional deficiencies". This includes material, calculation, design, production and installation deficiencies. This category of causes is of prime importance during the first 10 000 hours of operation in particular.

The second category we call "operational deficiencies". It includes operational and maintenance deficiencies and failure of supervisory, protective and control facilities. In this category we have also included failures due to wear andtear under operational conditions, such as erosion and corrosion.

The third category was designated "external influences". This includes failures originating in the boiler, in the oil supply system, in the generator and in the electric grid. Attention is drawn to the maxima at 10 000 and 20 000 hours of operation revealed by the guarantee inspections of the manufacturer on the one hand or the operational inspections by the operator and insurer on the other. The importance of timely inspection, which should be effected before the end of the first 10 000 hours of operation, is particularly clearly shown in this graph. Only in this way can productional deficiencies of a new steam turbine be discovered in time and eliminated.

Figure No. 2 shows the frequency of failure in the component "stator blades". Here, the straight-edged curve is almost identical with the idealised linearity of failure. This is due to greater clarity in recognition of the type of load on the stator blades. The completely different design

of the diaphragms in the action-type turbines most certainly also plays a role.

Figure No. 3 shows the evaluation for the nozzle category and Figure No. 4 that of the rotor blades of single-row action wheels. The rotor blades of the first stage in particular already show the striking figure of 50 % failure frequency upto 3 750 hours of operation. The stator blades of the nozzle category, on the other hand, show a clear increase in failure frequency, and thus a deviation from linear distribution, after approximately 20 000 hours of operation. Deeply latent productional deficiencies, such as sensitivity to thermal stresses, make their appearance here. Such cases of failure are usually first discovered in the course of inspections carried out during this operational period.

In Figure No. 5 particular attention is drawn to the category of failure causes known as "operational deficiencies" which occur much more frequently during the first period upto 12 500 hours of operation than in the previously shown Figures. During the initial period of operation, i. e. while the personnel operators are being trained and during replacement of the commissioning operators, experience shows that many errors in operation occur which in most cases lead to bearing failures. The sub-category "failure of protective facilities" contributes to this to a substantial degree, as essential protective facilities are, unfortunately, often insufficiently tested or not accurately adjusted due to lack of time during the starting-up period.

Figure No. 7 shows a similar trend. The majority of all failures to rotors occurs during the first 2 500 hours of operation solely as a result of errors made by the operators an failure of protective facilities, whereby the relative ex-

pansion and the vibration readings in particular play an important part. The category "productional deficiencies" mainly constitutes failures ensuing as a result of improper installation.

Figure No. 6 shows almost complete linearity in the failure frequency for cast-steel casings. "Productional deficiencies", especially material deficiencies, play a very important part after a considerable number of hours of operation.

Figure No. 8 shows the incidence of failures in respect of labyrinth seals. Conspicuous in this case again is the great number of errors on the part of the operator during the initial period of operation alone. The reappearance of this category of failure cause after 25 000 hours of operation should not give rise to confusion. These are mostly cases of failure resulting from wear and tear to the alloy-steel-strips of the labyrinth seals.

Figure No. 9 shows the failure incidence in respect of the control and stop valves of the steam turbines. The straight-edged curve differs from those previously shown in that it lies 100 % below the linear distribution. During the period up to 10 000 hours of operation, no serious valve failures are shown in our data. It is thus apparent that these components, which are of the utmost importance for the safe operation of steam turbines, have achieved a high degree of reliability. Only after a great number of hours of operation do latent design and - more frequently - latent material deficiencies in stems and valve seats make an appearance.

Looking through these graphs, the question automatically arises why only a limited period of approximately 41 000 hours of operation was evaluated. The reason for this is that the steam turbines with capacities of 100 MW and upwards selected by us achieve, on average, this particular number of hours of operation. Only very few turbo-sets manufactured during the initial period around 1957 - 1959 provide periods of operation exceeding this limit. In the period longer than 41 000 hours of operation, "operational deficiencies" and "external influences" are predominent. None of these categories of causes permit any true assessment of the reliability of component parts in steam turbines. On the other hand, evaluation should not be extended to older turbines of smaller capacity, because as the data gathered on these would be of no interest for future nuclear power plants. Aside from this the first five years of operation of a new turbo-set are today considered the most critical years of operation as regards reliability and availability, taking in account the desired base load of operation.

In conclusion, we should like to summarize the results in the last two Figures:

Figure No. 10 shows the probability of failure of the components mentioned, depending upon their hours of operation (a logarithmic scale was chosen for the presentation). For reasons of clarity, and in order to appease many critics of statistical processes right from the outset, the turbines were divided into those of the action-type and those of the reaction-type. Finally, a statistical coupling of both design types has been effected, with the result that a third column in the tables shows the values that may perhaps some day result for turbines of combined design. The results are a true criterion for the technical reliability of the individual components of steam turbines.

The rotor blades, the most feared components of steam turbines, reveal the greatest reliability. The reliability of the action-type turbine with heavier loads per blade-row is not, however, as good as that of the reaction-type turbine. Otherwise, there are no notable differences in the order of components, except for the fact that the cast-steel casings of the reaction-typee turbines are more ~~mmmmm kkmm~~ prone to damage than those of the action-type turbines. In this case, a special design may prove to be disadvantageous, or the larger dimensions of the cast-steel parts of reaction-type turbines may contribute.

In Figure No. 11 the abstract concept of technical reliability of a component is not based on its hours of operation, but rather upon the period of operation of the entire "steam turbine" unit. Thus, the importance of the rotor blades becomes immediately apparent. The rotor blades of both types of turbine design still represent a bottleneck as regards reliability or availability. The turbine of the action-type makes a pretty bad showing as far as evaluation of the rotor blades is concerned. This, however, is not surprising as here a decrease in the number of stages was particularly strongly associated with an increase in capacity from 150 MW to 300 MW per unit.

It should however, also appreciated that both constructional designs, with very little deviation, attain an increase in failure probability of the various components after 100 000 hours of operation. If these results are to be applied to the reliability evaluation of the components of the latest prototype turbines, then further parameters will have to be introduced into this statistical survey. The type of turbine and - for example - the load on the rotor blades will have to be considered as further criteria, since, as our data prove, they exert a major influence on the reliability of components.

On the subject of "causes of damage", the following summary is also presented:

The category "production deficiencies" is by far, the most important. Within this category, pure "design" and "calculation" errors play the more significant role. Material deficiencies have become very rare, and errors in installation are also very seldom found. This is quite apparently the result of improved material input controls and the use of qualified personnel for installation work, whereby supervision of the installation by the simultaneous employment of several erectionfitters and periodic inspections by the erection engineer-in-charge make the greatest contribution.

In the category "operational deficiencies", errors in operation are of consequence only during the initial working-up period, i. e. during the first two years of operation. In contrast to earlier data gathered and evaluated, favourable changes have been brought about by automation of the system and the almost complete protection afforded by supervisory facilities.

Undisputed first in the category of causes know as "external influences" are the breakdowns originating from live steam and reheated steam in conventional systems. Extremely serious failures have also resulted from breakdown in electric power mains.

Bibliography

FOGARTY, D. J. : Availability of Fossil-Fired Power Plants.
DER MASCHINENSCHADEN 39 (1966) H. 9/10, S. 129/140

MANDEL, H. : Große Blockeinheiten im Rahmen der deutschen Energieversorgung.
Mitteilung VGB 39 (1964), S. 247-257

VETTER, H. : Verfügbarkeitsuntersuchungen für Grundlastkraftwerke.
Mitteilung VGB 96 (1965), S. 185/91

SACK, M. : Die ersten 4 Betriebsjahre der 176 MW-Blöcke des Kraftwerks Westfalen der VEW.
ELEKTRIZITÄTSWIRTSCHAFT 67 (1968), H. 9, S. 224/232

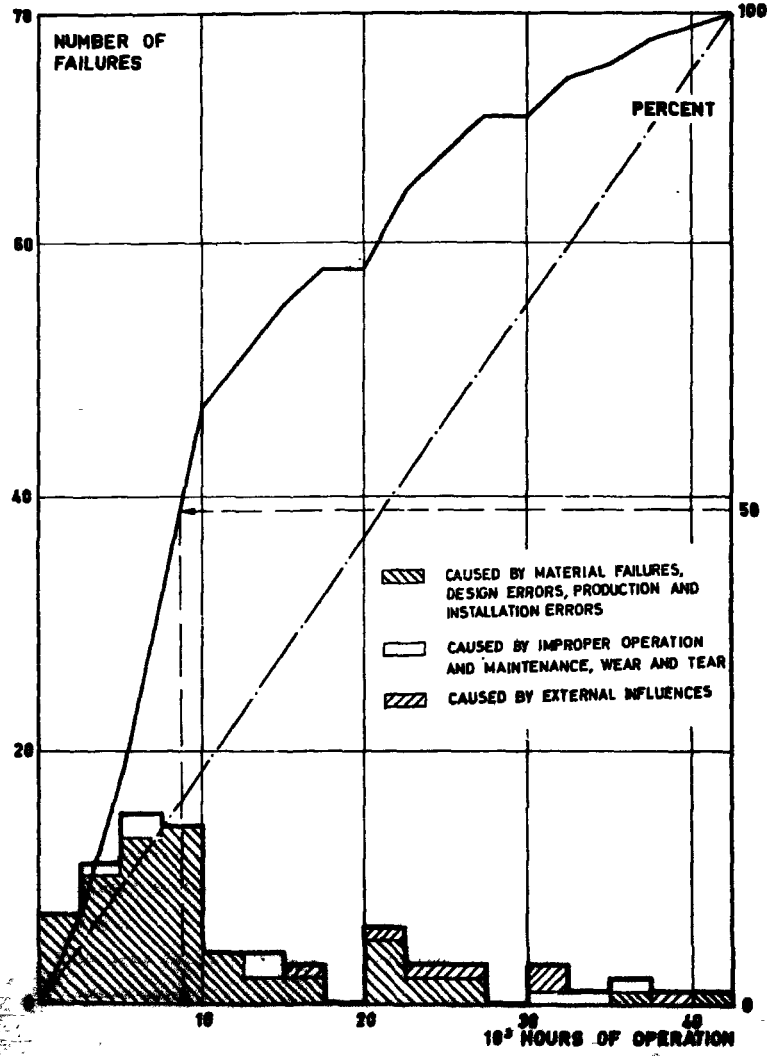
FELDMANN, J. : Auswertung von Schäden in Kernkraftwerken.
ATOMWIRTSCHAFT 14 (1969), H. 10

-.-.-.-.-

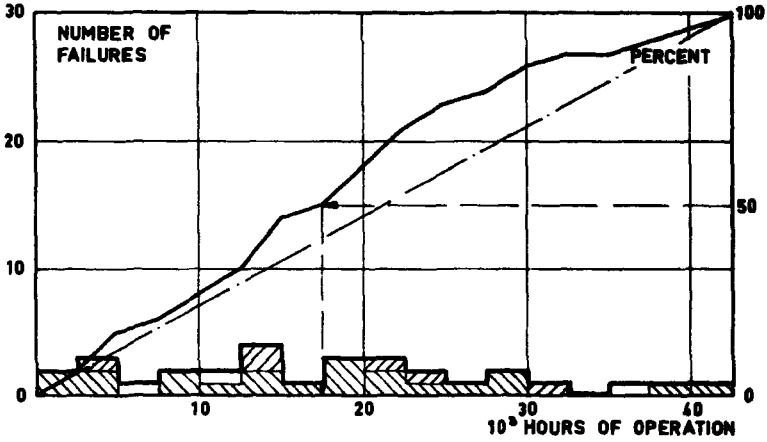
I should be pleased to answer any inquiries, which may arise in connection with this paper.

Address: Dipl.-Ing. H. HUPPMANN
ALLIANZ Versicherungs-Aktiengesellschaft
8000 München 22, Königinstraße 28
West-Germany

ROTOR BLADES



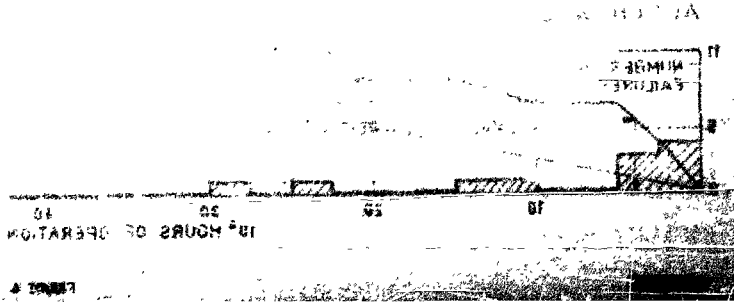
STATOR BLADES



CAUSED BY MATERIAL FAILURES, DESIGN ERRORS, PRODUCTION AND INSTALLATION ERRORS

CAUSED BY IMPROPER OPERATION AND MAINTENANCE, WEAR AND TEAR

CAUSED BY EXTERNAL INFLUENCES



NOZZLES

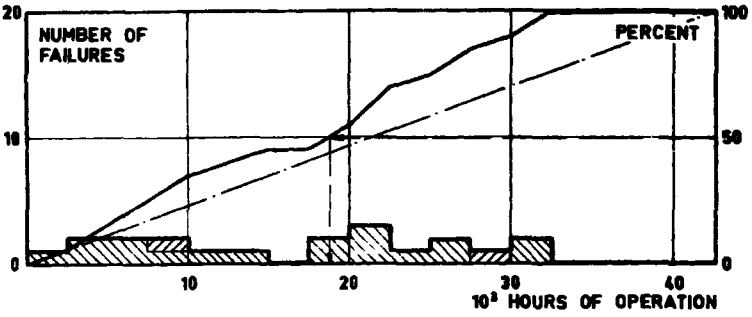


FIGURE 3

CAUSED BY MATERIAL FAILURES, DESIGN ERRORS, PRODUCTION AND INSTALLATION ERRORS

CAUSED BY IMPROPER OPERATION AND MAINTENANCE, WEAR AND TEAR

CAUSED BY EXTERNAL INFLUENCES

ACTION WHEELS

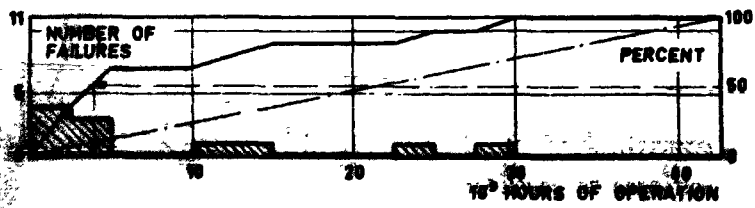
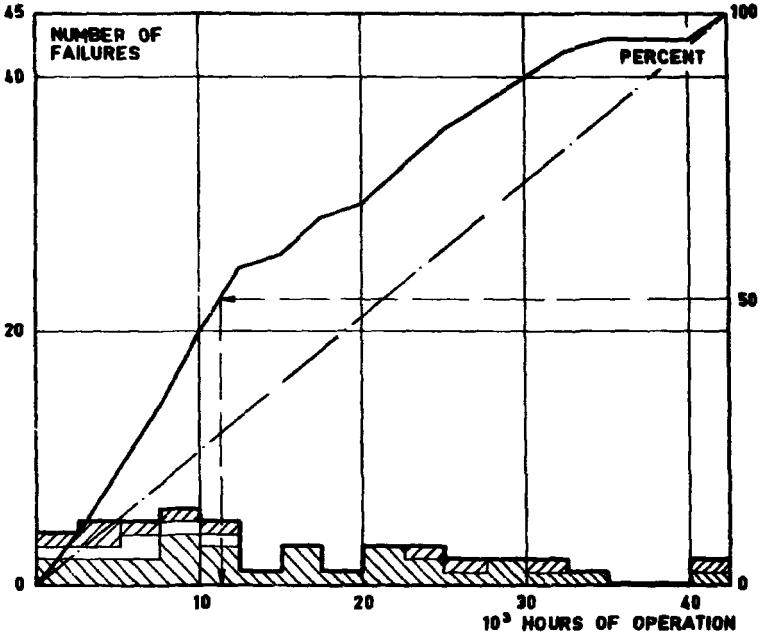


FIGURE 4

THRUST-, JOURNAL-BEARINGS



CASTSTEEL CASINGS

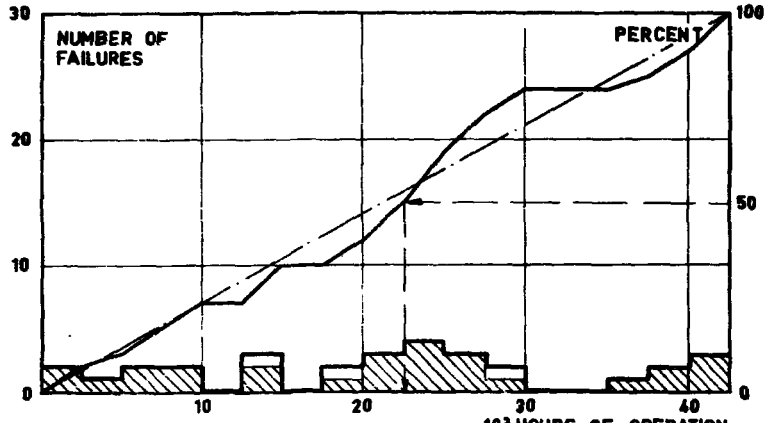


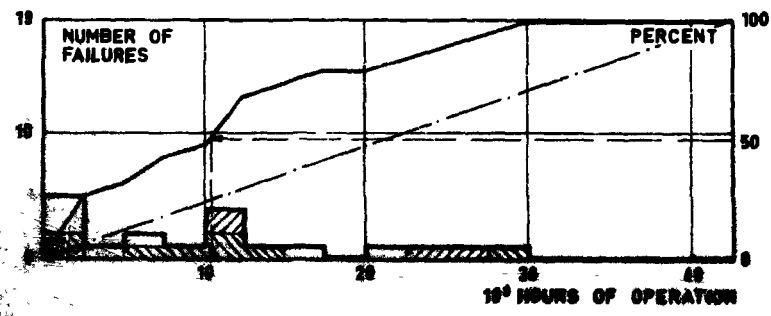
FIGURE 6

CAUSED BY MATERIAL FAILURES, DESIGN ERRORS, PRODUCTION AND INSTALLATION ERRORS

CAUSED BY IMPROPER OPERATION AND MAINTENANCE, WEAR AND TEAR

CAUSED BY EXTERNAL INFLUENCES

ROTORS



SEALS

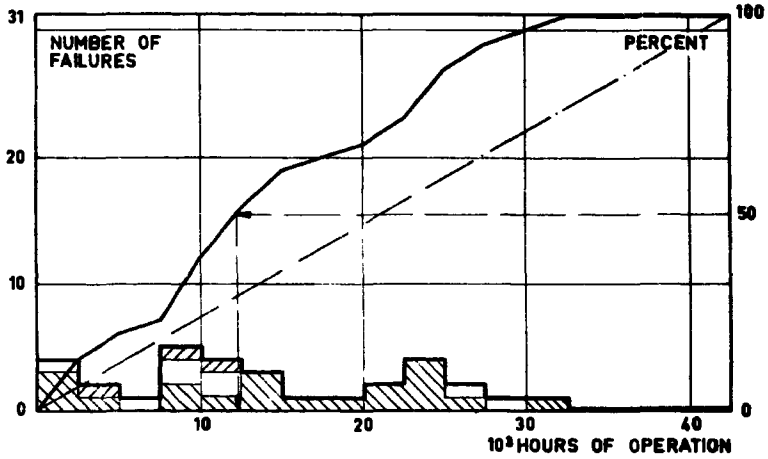


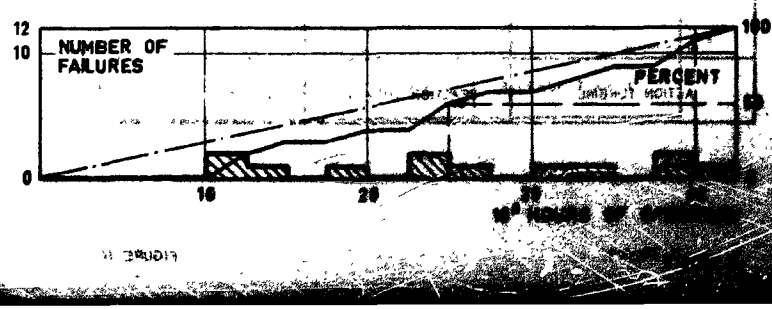
FIGURE 8

CAUSED BY MATERIAL FAILURES, DESIGN ERRORS, PRODUCTION AND INSTALLATION ERRORS

CAUSED BY IMPROPER OPERATION AND MAINTENANCE, WEAR AND TEAR

CAUSED BY EXTERNAL INFLUENCES

VALVES



PROBABILITY OF FAILURE FOR SELECTED COMPONENTS OF STEAM TURBINES WITH REFERENCE TO THE HOURS OF OPERATION OF THE COMPONENTS

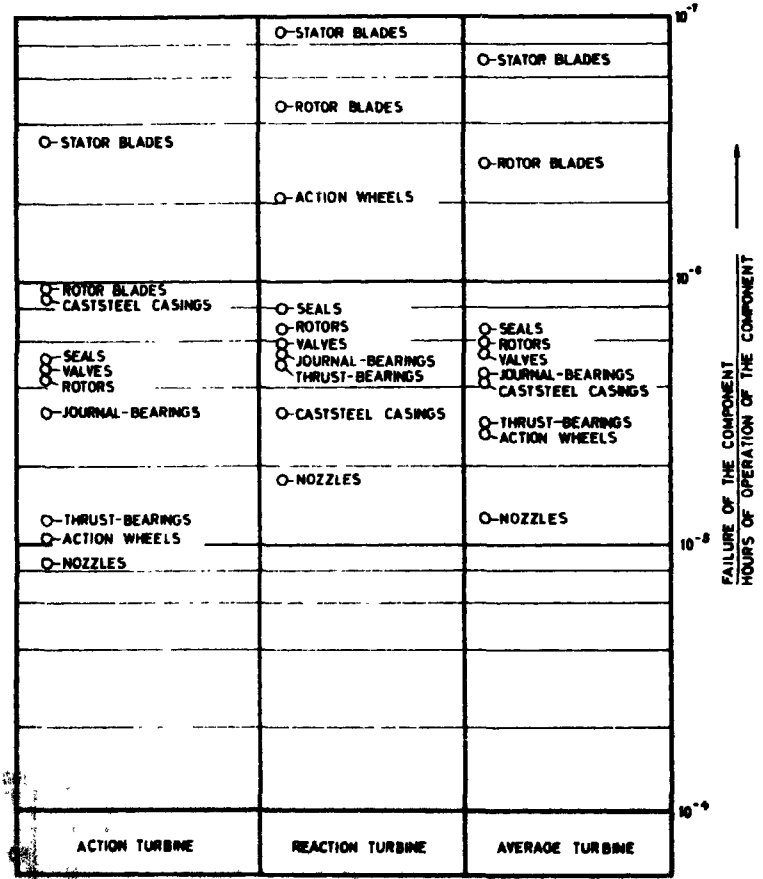
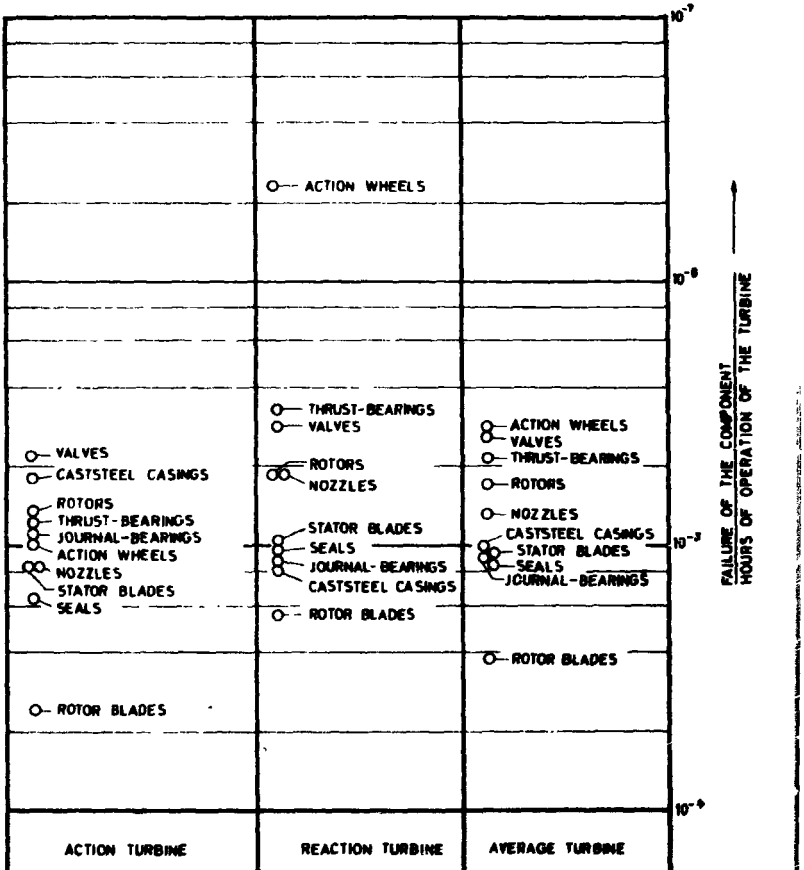


FIGURE 10

PROBABILITY OF FAILURE FOR SELECTED COMPONENTS OF STEAM TURBINES WITH REFERENCE TO THE HOURS OF OPERATION OF THE TURBINE



La minimisation de la somme U conduit à une expression des a_r^0, a_r^1,..., a_r^n à partir d'opérateurs de lissage S_r^0, S_r^1, ..., S_r^n définis par la relation de récurrence $S_r^n(X) = \alpha S_r^{n-1}(X) + (1-\alpha) S_{r-1}^n(X)$ avec $S_r^0(X) = X_r$.

La valeur du MTBF estimée après la panne de rang r est alors donnée par :

$$MTBF(t) = a_r^0 + a_r^1 (t - tr) + \dots a_r^n (t - tr)^n$$

l'origine des temps choisie étant celle de la dernière panne.

Dans la pratique, une tendance parabolique est choisie, ce qui conduit à un triple lissage.

Un programme de calcul permettant d'effectuer les calculs numériques a été mis au point.

La constante de lissage α est, par définition, un nombre compris entre zéro et un. L'auteur de la référence 3 signale, qu'en général, les meilleurs résultats sont obtenus en choisissant la constante entre 0,1 et 0,3. Ce renseignement n'est qu'indicatif et, dans la pratique, on détermine par un étalonnage du procédé de lissage sur la partie de la chronique qui est connue.

Formuler une estimation prévisionnelle du MTBF n'a de valeur que si on peut fixer un intervalle de confiance à l'estimation faite et si un moyen d'alerte assez sensible permet de signaler un changement dans le comportement du système étudié.

L'erreur de prévision peut être définie comme la différence entre la prévision et la réalisation :

$$e_r = TBF(tr) - \widehat{MTBF}(tr)$$

Si le modèle choisi représente bien le processus de croissance du MTBF, la moyenne des erreurs est nulle et la distribution des erreurs est normale.

Pour fixer la précision de la prévision, il faut calculer la variance ou l'écart type de la distribution des erreurs σ. Une solution plus simple consiste à définir la dispersion de la distribution des erreurs non par son écart type mais par son écart moyen δ (pour une loi normale $\delta = \sqrt{\frac{2}{\pi}}\,\sigma \approx \frac{\sigma}{0,8}$).

Une estimation continue de σ, $\hat{\delta}_r = \hat{\delta}(tr)$ s'obtient par un simple lissage de la série des erreurs qui doit être stationnaire et de moyenne nulle.

Les limites de confiance se calculent alors à partir de la valeur prévisionnelle de δ, $\hat{\delta}(tr)$, l'on a :

$$MTBF\,(tr + \tau) = \widehat{MTBF\,(tr + \tau)} \pm \frac{K\,\hat{\delta}_r}{0,8}$$

Si l'on veut un intervalle de confiance bilatéral à 95 %, une table de la loi normale réduite indique que K est égal à 1,96.

De plus, un signal d'alerte peut consister à vérifier, en permanence, si la somme algébrique des erreurs fluctue effectivement bien autour de zéro. On peut le vérifier, qualitativement, en traçant d'une façon continue la somme des erreurs. Pour faire une estimation quantitative qui permet seule la prise de décision, il est nécessaire de calculer la variance de la somme des erreurs.

Le programme de calcul de lissage établi permet de calculer la variance des erreurs ainsi que la variance de la somme des erreurs et par conséquent de juger de la validité des $\widehat{MTBF}\,(t^0)$ obtenus.

AGENCE EUROPEENNE POUR L'ENERGIE NUCLEAIRE
COMITE DES TECHNIQUES DE SECURITE DES REACTEURS

Réunion de spécialistes en matière de fiabilité
des composants et des systèmes mécaniques
destinés à assurer la sécurité des réacteurs

"FIABILITE OPERATIONNELLE D'UNE MACHINE - FIABILITE PREVISIONNELLE D'UN SYSTEME COMPRENANT N MACHINES EN PARALLELE"

par

P. MICHEAU*

et

A. HENNEBIQUE**

* Société BERTIN - Boîte Postale n° 3 - 78 PLAISIR.
** ELECTRICITE DE FRANCE - Boîte Postale n° 26 - 37 TOURS.

1 - INTRODUCTION

Les constructeurs de systèmes mécaniques ont, de tout temps, cherché à conférer à leurs fabrications une sûreté de fonctionnement satisfaisante.

Mais, il n'y a que récemment qu'on a cherché à quantifier cette sûreté de fonctionnement.

Ce besoin a donné naissance à la fiabilité mécanique qui est caractérisée par :

- la difficulté d'obtenir des résultats statistiques significatifs, les systèmes étant généralement construits en nombre restreint,
- l'existence d'interactions difficile à préciser entre les composants d'un système,
- la possibilité d'effectuer des réparations.

Après avoir rappelé quelques généralités sur la fiabilité, on expose :

- les méthodes permettant, à partir de résultats d'essais, de calculer la fiabilité opérationnelle d'une machine réparable et la fonction de répartition des durées d'arrêt correspondante,
- une méthode de calcul de la fiabilité prévisionnelle d'une fonction assurée par N machines associées en parallèle et supposées sans interaction.

Cette étude a été effectuée pour le compte de l'Electricité de France et les méthodes décrites appliquées au calcul de la fiabilité de la fonction soufflage du réacteur Saint Laurent 1 de la centrale nucléaire de SAINT-LAURENT-DES-EAUX.

2 - GENERALITES

La fiabilité de sûreté de fonctionnement d'un système est la probabilité que ce système fonctionne de façon satisfaisante pendant une durée dornée et dans des conditions d'utilisation précisées.

La fiabilité d'un système peut être calculée au stade du projet - fiabilité prévisionnelle - et/ou déterminée expérimentalement, la réalisation une fois achevée - fiabilité opérationnelle -.

Dans le premier cas, il est fait appel aux règles du calcul de fiabilité issues du calcul des probabilités et aux données numériques relatives aux organes composants. Ces données sont issues de l'expérience industrielle antérieure ou d'essais systématiques de laboratoire. Ce genre de renseignement de plus en plus fréquemment communiqué par les fournisseurs de composants électroniques l'est encore bien rarement, pour ne pas dire jamais, dans le domaine de la mécanique.

Dans le second cas, on fait appel à des techniques statistiques utilisées aussi en contrôle de qualité (tests séquentiels, tests tronqués, tests accélérés, etc...) qui permettant soit de confirmer les valeurs des fiabilités adoptées ou calculées au stade du projet, soit de fournir de nouvelles valeurs plus réalistes.

2.1. - Définitions mathématiques

Mathématiquement, on définit la fonction fiabilité d'un système, $F(t)$, ou fonction de survie comme la distribution cumulée des probabilités de bon fonctionnement de ce système.

La densité de panne d'un système, f (t), est la probabilité de panne entre les instants t et t + dt ; on a évidemment :

$$\int_0^\infty f(t)\,dt = 1 \quad \text{et} \quad F(t) = \int_t^\infty f(t)\,dt$$

d'où :

$$f(t) = -\frac{dF}{dt}$$

La taux de panne ou taux d'avarie est égal à $\frac{f(t)}{F(t)}$. C'est la probabilité conditionnelle d'avarie à l'âge t d'un matériel ayant vécu jusqu'à cet âge. Dans le cas général, le taux de panne varie avec le temps.

2.2. - Modèles

L'expérience montre que la vie d'un composant ou d'un système peut être décomposée en trois périodes :

- une période dite d'apprentissage ou de jeunesse pendant laquelle apparaissent des pannes aléatoires et des pannes systématiques, les dernières étant dues à des défauts de mise au point, à un certain nombre de composants plus faibles que la normale, etc... On pallie ces défauts de jeunesse, et, pendant cette première période, on constate un taux de panne décroissant ;

- une période dite de vie utile où les pannes se produisent à des instants aléatoires mais avec un taux moyen constant. La moyenne des temps de bon fonctionnement m ou MTBF, $m = \frac{1}{\lambda}$, est aussi constante ;

- une période dite d'usure où certaines pannes sont aléatoires et d'autres causées par l'usure. Le taux d'avarie est croissant.

Ces considérations, sur le taux de panne, sont généralement résumées par une courbe dite en baignoire qui représente le taux d'avarie λ en fonction du temps (Cf. figure 1).

- dans la zone (2) où λ est une constante, la densité de panne et la loi de survie sont des exponentielles (figures 2, 3).

$$F(t) = e^{-\lambda t} \qquad f(t) = \lambda e^{-\lambda t}$$

- dans la zone (3), la densité de panne est généralement une loi normale symétrique autour du temps M qui correspond à une moyenne de durée de vie (Cf. figures 4 et 5).

Dans le cas qui nous intéresse, le système à étudier est composé de P machines réparables fonctionnant en parallèle. Pour déterminer la fiabilité prévisionnelle du système, il est nécessaire de connaître la fonction de fiabilité opérationnelle ou prévisionnelle et la fonction de répartition des durées d'arrêt, pour chaque machine.

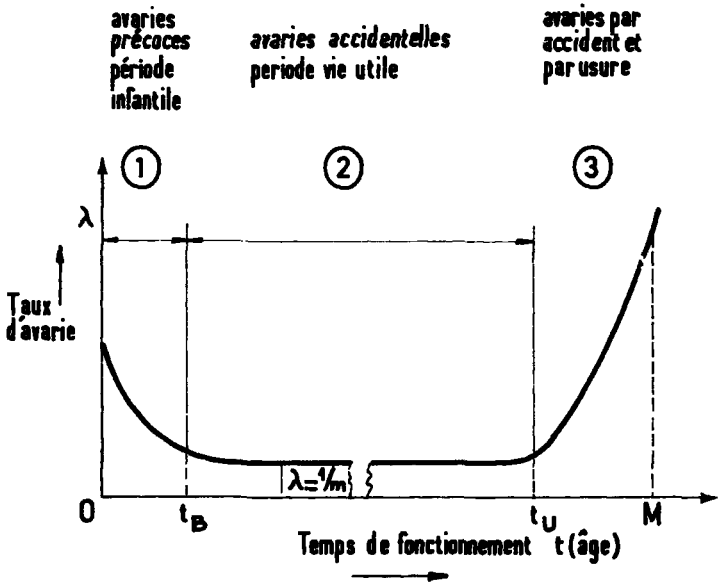

avaries précoces période infantile
avaries accidentelles periode vie utile
avaries par accident et par usure
1
2
3
λ
Taux d'avarie
λ=1/m
0
t_B
t_U
M
Temps de fonctionnement t (âge)

Figure 1

Vie utile

Fiabilité accidentelle

$$\frac{dF}{dt} = -\frac{1}{m}F(t)$$

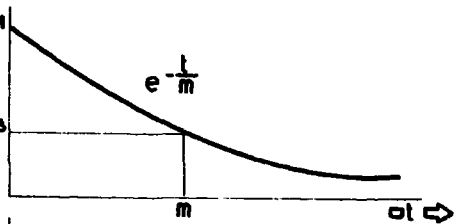


Fig. 2

$$f(t) = -\frac{dF(t)}{dt}$$

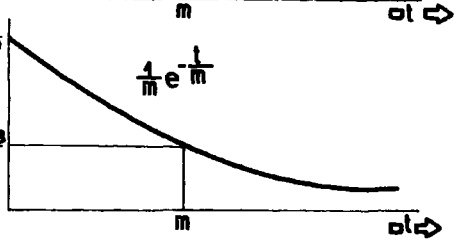


Fig. 3

Période d'usure

Fiabilité d'usure

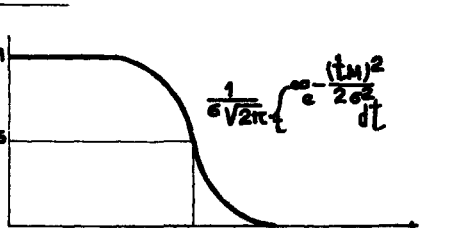


Fig. 4

$$f(t) = -\frac{dF(t)}{dt}$$

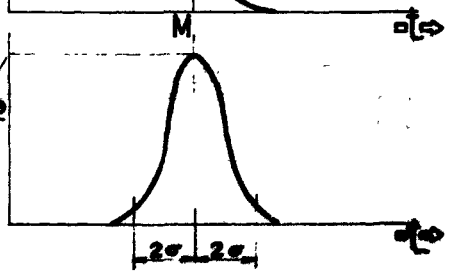


Fig. 5

3 - FIABILITE OPERATIONNELLE, FONCTION DE REPARTITION DES DUREES D'ARRET D'UNE MACHINE

3.1. - Fiabilité opérationnelle pendant la période d'essai

On montre (Réf. 1) et, comme on l'a déjà dit, on vérifie expérimentalement que, dans le cas d'un système complexe où les sources de panne sont nombreuses, indépendantes et où, aucune de ces sources n'est prépondérante, la loi de fiabilité est une exponentielle. Le taux de panne est alors constant et égal à l'inverse de la durée moyenne de bon fonctionnement (MTBF).

Si cette affirmation est vraie, pour un système au point, elle est partiellement inexacte pour un système en cours de mise au point, pendant la phase dite d'apprentissage ou pour un système qui entre dans la phase d'usure.

Dans ces deux cas, les taux de panne sont respectivement décroissant et croissant. On peut admettre, dans ces cas, que le taux de panne est constant seulement pendant des intervalles de temps limités.

Nous admettons que la politique de maintenance permet d'écarter le cas de l'usure. Si il n'en était pas ainsi, à partir d'un certain moment, on constaterait effectivement une croissance du taux de panne puis sa stabilisation à un niveau élevé, la loi de fiabilité de la machine restant de forme exponentielle.

Mais revenons à la phase d'apprentissage.

Suite aux corrections apportées aux lacunes initiales du système, le taux de panne décroît. On admet que la loi de fiabilité du système est toujours une exponentielle mais avec un taux de panne (ou un MTBF) qui n'est constant que localement.

L'estimation de la valeur du MTBF, dans la phase d'apprentissage, présente alors quelques difficultés. En effet si, comme a pu le montrer EPSTEIN (Réf. 1), la moyenne arithmétique des temps de bon fonctionnement est le meilleur estimateur du MTBF lorsque le taux de panne est constant, c'est aussi le plus mauvais lorsque ce paramètre évolue.

Pour surmonter cette difficulté, on considère la suite des durées de bon fonctionnement - TBF (t) - comme une série chronologique que l'on traite par une méthode de lissage exponentielle de BROWN (Réf. 3 et 4).

Dans le cas d'une telle chronique, on peut formellement distinguer, pendant la phase d'apprentissage, deux termes : un terme de tendance MTBF (t) = $\overline{TBF}$ (t) et un terme d'aléa dont la présence obscurcit la tendance.

$$TBF(t) = \overline{TBF}(t) + e(t)$$

Soit X_r la suite des durées de bon fonctionnement (r rang des pannes). L'originalité de la méthode exponentielle réside en le fait qu'une fois choisi le modèle de la tendance, sous forme polynomiale par exemple :

$$MTBF = \overline{TBF}(t) = a^0 + a^1 t + \ldots + a^n t^n,$$

l'estimation des a_0, a_1, a_n, après la panne de rang r,

$$- \mathfrak{a}^0_r,\ \mathfrak{a}^1_r,\ \ldots\ \mathfrak{a}^n_r$$

se fait non pas en minimisant la somme $\sum_{p=1}^{r} (X(p) - \hat{X}(p))^2$ mais en minimisant la somme $U = \sum_{p=1}^{r} (1-\alpha)^{2(r-p)} (X(p) - \hat{X}(p))^2$ ceci avec l'objectif d'accorder, pour la prévision, aux écarts prévision-réalisation les plus récents une importance plus grande qu'aux plus anciens.

3.2. - Fiabilité à la fin de la période d'essai

Le calcul de la fiabilité prévisionnelle d'une fonction assurée par un groupe de machines, sans interaction associées en parallèle, peut être conduit à partir de la fiabilité opérationnelle de chaque machine en cours d'essai, c'est-à-dire en période infantile. Mais, il paraît souhaitable de pouvoir disposer de la fiabilité opérationnelle de chaque machine pendant la période de vie utile.

La méthode présentée par Martin H. SALTZ au 5ème Symposium National sur la fiabilité et le contrôle de qualité, en 1959 à Philadelphie permet, entre autres, le calcul de cette fiabilité à partir des résultats d'essais de mise au point (Réf. 5).

On admet que le système a une fiabilité exponentielle et on avance l'hypothèse que les pannes appartiennent à deux familles :

- une famille de pannes dites primaires, peu nombreuses, ayant une forte probabilité d'arrivée et auxquelles il correspond une moyenne de temps de bon fonctionnement $MTBF_p$,

- une famille de pannes secondaires, nombreuses, ayant une faible probabilité d'arrivée et auxquelles correspond une moyenne de temps de bon fonctionnement $MTBF_s$.

On suppose que les sources de pannes primaires peuvent être détectées et corrigées pendant la période de mise au point et qu'elles ne se manifesteront plus par la suite. On suppose également que la correction d'une source de pannes primaires ne modifie pas le taux de pannes dû aux pannes secondaires.

Ainsi, une fois toutes les causes d'avaries primaires éliminées, le taux de panne devient constant et égal au taux de panne, $MTBF_s$, conséquence des avaries secondaires seulement. Ce taux de panne est le plus faible que l'on puisse espérer lorsque le système sera au point.

Le matérial doit être essayé dans les conditions assez proches de l'exploitation normale. La fiabilité dépend du niveau de contraintes ou mode de fonctionnement.

Le $MTBF_s$ est tout au long de la période d'essai une constante alors que le $MTBF_p$ peut varier par paliers lorsque les réparations correspondant aux pannes primaires modifient la machine.

La courbe "moyenne" donnant les durées cumulées des temps de bon fonctionnement t en fonction du rang des pannes est ainsi une succession de segments de droite, correspondant aux pannes primaires, avec en plus un certain nombre de points, correspondant aux pannes secondaires ($MTBF_p \ll MTBF_s$).

La méthode de dépouillement des résultats expérimentaux permettant de calculer le $MTBF_s$ découle immédiatement de cette remarque.

1) On trace la courbe donnant les temps de bon fonctionnement cumulés en fonction du rang des pannes,

2) On assimile grossièrement chaque portion, sans cassure, de cette courbe à des segments de droite correspondant aux périodes Δt_i où la machine n'a pas subi de modifications provenant de la réparation de pannes primaires.

Pendant les périodes Δt_i, le nombre de pannes est ΔP_i.

3) On choisit un $MTBF_s$.

4) On calcule pour chaque période Δt_i, le $(MTBF_p)_i$

$$(MTBF_p)_i = \frac{\Delta t_i}{\Delta P_i - \frac{\Delta t_i}{MTBF_s}}$$

5) On détermine les dates $\hat{t}$ d'apparition "en moyenne" des pannes en fonction de leur rang

$(MTBF_p)_1$, 2 $(MTBF_p)_1$, ... $MTBF_s$, ..., $(r MTBF_p)_1$, r $(MTBF_p)_1$

+ $(MTBF_p)_2$, r $(MTBF_p)_1$ + p $(MTBF_p)_2$ .....

6) On calcule la somme $\sum_1^n (tr - \hat{tr})^2$ pour toute la période d'observation disponible.

La bonne valeur du $MTBF_s$ est celle qui minimise la somme $\sum(t - \hat{tr})^2$, ce qui peut se déterminer graphiquement.

3.3. - Répartition des durées d'arrêt

L'étendue des valeurs des durées d'arrêt étant généralement faible par rapport au temps de bon fonctionnement, on adopte par souci de simplicité une loi exponentielle pour la fonction de répartition des durées d'arrêt d'une machine.

Le paramètre définissant cette loi est obtenu par ajustement graphique à partir des résultats d'essais. Aucune discrémination n'est effectuée entre les pannes primaires et les pannes secondaires.

4 - FIABILITE PREVISIONNELLE D'UNE FONCTION

4.1. - Plusieurs machines peuvent être réparées simultanément

Dans ce qui suit, on admet qu'une fonction assurée par un ensemble de machines supposées sans interaction, associées en parallèle, est remplie lorsqu'une au moins des machines est en état de marche.

A partir de la fiabilité opérationnelle de chaque machine et de la loi de répartition des durées de panne correspondante obtenues en cours d'essai, on peut calculer la fiabilité prévisionnelle de la fonction considérée :

- soit analytiquement, on obtient alors directement la fonction fiabilité,
- soit par une méthode de simulation représentant le fonctionnement réel, pendant une période T, de N fonctions, on obtient alors le nombre n_i de fonctions échantillons encore en vie aux instants t_i.

Dans ce dernier cas, il est :

- soit possible de déterminer la fonction fiabilité cherchée par ajustement graphique à partir du graphe $(\frac{n_i}{N}, t_i)$; la fiabilité déterminée est dite paramètrique,
- soit nécessaire d'utiliser pour déterminer la fiabilité les résultats relatifs aux tests tronqués, ne disposant pas d'assez de points $(\frac{n_i}{N}, t_i)$; la fiabilité déterminée est dite non paramètrique.

Nous avons choisi une méthode de simulation du type "Monte-Carlo" et nous avons dû calculer une fiabilité non paramètrique.

Pour simuler le fonctionnement réel, il s'agit de déterminer, au hasard, pour chaque machine échantillon, des durées de marche et d'arrêt qui, bien qu'aléatoires, doivent respecter les lois de survie et d'indisponibilité choisies.

On démontre que l'on atteint ce résultat en tirant au hasard des nombres a_i compris entre 0 et 1, puis en faisant correspondre, par l'intermédiaire des lois de fiabilité de répartition des durées de répartition à chaque nombre a_i des durées de vie ou de réparation t_{fi} et t_{ri} (figure 6). En alternant les périodes de marche et d'arrêt pour chacune des machines et en poursuivant l'opération jusqu'au temps voulu, on obtient l'histoire de la fonction soufflage que l'on peut illustrer par la figure 7. Sur cette dernière, il est facile de comptabiliser la fréquence des évènements qui présentent de l'intérêt pour le problème posé.

Deux programmes de calcul existent qui permettent de faire cette simulation.

Le premier programme, assez simple, a été écrit dans le but d'obtenir rapidement des résultats.

Il permet de faire fonctionner N fois quatre machines identiques (N fonctions) pendant un temps T quelconque, chaque machine étant réparée dès qu'elle tombe en panne. La loi de fiabilité et la fonction de répartition des durées de *répartition de la machine type sont des exponentielles. Les dates d'apparition* du premier arrêt simultané des quatre machines sont ensuite données.

Le deuxième programme est d'utilisation plus générale :

- le nombre de machines constituant la fonction globale et le nombre de simulations peuvent être librement choisis (sous réserve des limitations dans la dimension des tableaux et l'encombrement en mémoire centrale de l'ordinateur utilisé),

- les machines sont individualisées (chaque machine a ses lois propres et un âge indépendant de celui des autres),

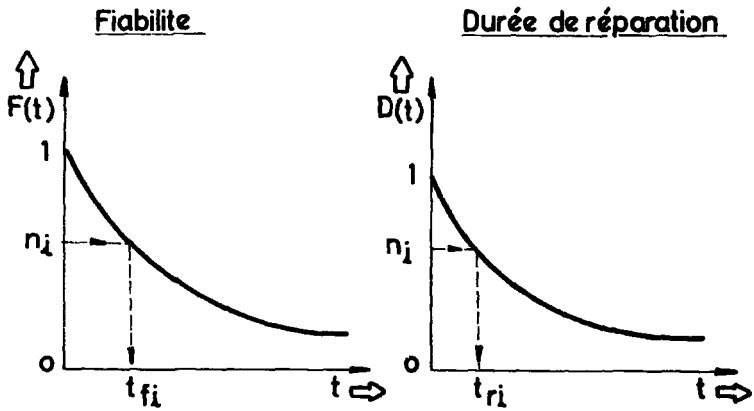


Figure 6

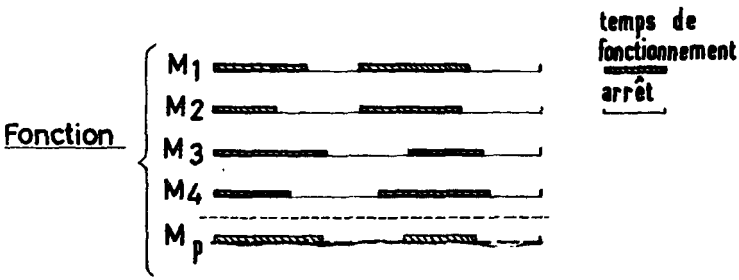


Figure 7

- les différents états successifs de la fonction globale, leur date d'apparition et leur durée sont maintenus en mémoire.

Cette dernière option permet en particulier de connaître :

- les dates d'apparition des premières "pannes" (plus exactement les dates des premières séquences comportant 0, 1, 2 ..... machines en panne), d'où l'estimation de la fiabilité,

- la répartition de ces séquences en classes successives de durées (durées probables de fonctionnement ou d'arrêt), d'où connaissance de la disponibilité. Le nombre d'évènements possible étant très grand, les résultats ne fournissent pas toutes les durées correspondantes individualisées mais groupées en classes. Le nombre de ces classes a été choisi égal à 12. Les durées des évènements (panne ou bon fonctionnement) pouvant varier à l'intérieur de limites très vastes (quelques minutes à des centaines de millier d'heures), les intervalles de classes n'ont pas été pris équidistants mais espacés, suivant une progression géométrique. Cette loi de répartition est modifiable à volonté au niveau des données.

Connaissant à un instant t le nombre de fonctions échantillons tombées en panne : N - n, on estime (Réf. 6, 7) une limite inférieure de la fiabilité au bout du temps t correspondant à un intervalle de confiance unilatéral à 100 $(1 - \alpha)$ à l'aide de la relation

$$\hat{F}(t) = \frac{1}{1 + \left(\frac{N - n + 1}{n_1}\right) \mathcal{F}_{\alpha\,;\,2(N-n)+2\,;\,2n}}$$

où $\mathcal{F}_{\alpha\,;\,2(N-n)+2\,;\,2n}$ correspond à la valeur au seuil α de la distribution du $\mathcal{F}$ avec les degrés de liberté indiqués. Cette estimation de la fiabilité permet donc d'affirmer qu'il y a une probabilité $1 - \alpha$ d'avoir une fiabilité pour t heures supérieure ou égale à la valeur $\hat{F}(t)$. Comme déjà

signalé, il s'agit là d'une *estimation non paramètrique valable que le comportement de la fonction étudiée soit du type exponentiel ou non.*

4.2. - Une seule machine peut être en réparation à chaque instant

Outre la fiabilité d'une fonction précédemment définie et calculée, il est intéressant de pouvoir déterminer la fiabilité de la fonction lorsque 1, 2, p machines sur les P machines, associées en parallèle pour assurer la fonction, sont en panne et ne peuvent être réparées. Ce cas se présente lorsqu'on ne peut réparer qu'une machine à la fois, la fonction étant alors assurée par les N - 1 machines restantes.

Si l'on suppose les machines identiques, de fiabilité F (t), la fiabilité d'une telle fonction est alors donnée (Réf. 6) par la somme des termes du développement du binome

$$(F(t) + D(t))^{N-1} = F(t)^{N-1} + C_{p-1}^{1} F(t)^{N-2} D(t) \ldots$$

avec D (t) = 1 - F (t)

et où :

- $F(t)^{(N-1)}$ est la probabilité de voir survivre (N - 1) machines jusqu'à l'instant t,

- $C_{p-1}^{1} F(t)^{P-2} D(t)$ la probabilité de voir survivre (N - 2) machines, etc...

Si la fiabilité de la fonction est toujours définie comme l'existence d'une seule machine en service, elle est alors égale à $C_{p-1}^{1} F(t) D(t)$. Dans le cas où les machines assurant la fonction ne sont pas identiques, la fiabilité de la fonction s'obtient à partir du développement de l'expression :

$$\prod_{i=1}^{P=1} (F_i(t) + D_i(t))$$

$F_i(t)$ étant la fiabilité opérationnelle de la machine du rang i et $D_i(t)$ égal à $1 - F_i(t)$.

5 - CONCLUSION

Dans l'exposé qui précède des méthodes permettant de calculer à partir de résultats d'essai durant la période infantile, la fiabilité opérationnelle de machines considérées comme des boîtes noires ont été développées.

Puis une méthode de simulation permettant de calculer une fiabilité prévisionnelle d'une fonction assurée par l'association en parallèle de plusieurs machines supposées sans interaction a été indiquée.

L'inconvénient de cette méthode est qu'elle permet seulement de calculer une fiabilité non paramétrique.

Il serait intéressant de comparer sur les exemples traités les résultats obtenus avec ceux que donnerait une méthode de calcul analytique (Réf. 8 et 9).

REFERENCES

1. The reliability of repairable systems
by George MAGY
Goodyear Aircraft Corporation - AKRON - Ohio
Natural Symposium on Reliability and Quality Control
January 1967

2. Statistical life test acceptance procedures
by B. EPSTEIN
Technometrics 2, Novembre 1960

3. Exponential smoothing for prediction of reliability growth
by Thomas L. PAGAN and Myron A. WILSON
Missile and Space Division, General Electric Cº
Philadelphia-Pennsylvania

4. La prévision économique à court terme
Méthodes générales - Lissage exponentiel
par H. KAUFMAN et J.L. GROSCHLOT
Dunod 1968

5. Methods for evaluating reliability growth an ultimate reliability during development of a complex system
by Martin H. SALTZ
Head, reliability analysis, guided missile laboratories,
Hughes Aircraft Company Culver City, California
5th National Symposium on Reliability and Quality Control Philadelphia
(January 12-14, 1959)

6. Fiabilité - Théorie et pratique de la sûreté de fonctionnement
par I. BAZOVSKY
Dunod 1966

7. Statistical theory with engineering applications
by A. HALD
John WILEY and Sons, in 1952

8. Reliability of parallel systems with repair and switching
by S.G. KNEALE
Chief of Technical Analysis and Planning Electronics Division
Avco Corporation Cincinnati, Ohio
7th National Symposium on Reliability and Quality Control
(January 9-11, 1961)

9. Reliability of non exponential redundant systems
by R.A. HALL, H. HUBNER, Dr. L.B. ANNER
Computa Applications Inc., New York, N.Y. and F.N.
Stehle Bureau of Ships, Washington D.C.

AUSLEGUNG UND ANORDNUNG EINER REAKTOR-BESCHICKUNGSANLAGE AUFGRUND VON ZUVERLÄSSIGKEITSBETRACHTUNGEN

U. Hennings
BROWN BOVERI / KRUPP Reaktorbau GmbH
Mannheim

Für ENEA/CREST-EURATOM-UKAEA
Fachtagung über Zuverlässigkeit mechanischer
Komponenten und Systeme
für die Sicherheit von Kernreaktoren

Riseo. 24.-26. September 1969

AUSLEGUNG UND ANORDNUNG EINER REAKTOR-BESCHICKUNGSANLAGE AUFGRUND VON ZUVERLÄSSIGKEITSBETRACHTUNGEN

U. Hennings

Brown Boveri/Krupp Reaktorbau GmbH
68 Mannheim

Zusammenfassung

Ein Reaktorkern von 300 MWe Leistung, der rund 700.000 bewegte kugelförmige Brennelemente enthält, braucht eine besondere Beschickungsanlage. Diese ist beim Kugelhaufenreaktor außerhalb des Kerns angeordnet und täglich in Betrieb. Sie muß außer der Kugelbewegung und Zuordnung zu Core-Zonen auch die jeweils vorhandenen physikalischen und mechanischen Eigenschaften der Kugelelemente bei äußerem Durchlauf, bei einer Kugelfolge von ca. 7 Sekunden, feststellen. Wenn auch der Reaktor bei vorübergehendem Stillstand der Beschickungsanlage volle Leistung produzieren kann, ist bei der Auslegung dieser Einrichtung mit ihren dynamisch beanspruchten Bauteilen die Zuverlässigkeit besonders zu beachten. Die Analyse zeigt, daß, auch unter der pessimistischen Annahme einzelner Imponderabler Schäden, Verfügbarkeiten von 99,4 % = insgesamt ca. 60 Tage Ausfall, wie verlangt, erreicht werden. Mit weitergehender Redundanzanordnung wären Ausfallzeiten von 19 oder gar 0,9 Tagen erreichbar. Hierfür wären jedoch die Mehrkosten für Anlage und Wartung größer als der Gewinn durch Verfügbarkeit.

Beschreibung der Anlage

Im Gegensatz zu Reaktoren mit stabförmigen Brennelementen erfordert der Kugelhaufenreaktor keinerlei Maschinen für die Brennstoffbeschickung, -umsetzung oder -entnahme innerhalb des Reaktorkerns. Für die Abwärtsbewegung von Kugeln

wird die Schwerkraft ausgenutzt, pneumatische Energie wird für die Aufwärtsbewegung und damit Zugabe oder das Umwälzen von Brennelementen verwendet. Die einzigen Bestandteile der Beschickungsanlage am Core sind Rohre, die an entsprechenden Punkten der Core-Peripherie angeordnet sind. Sämtliche Verrichtungen, um die gewünschte Kugelbewegung, die Kugelinspektion und die Zugabe oder den Abzug von Brennelementen auszuführen, sind unterhalb des Kerns und dessen Druckbehälter angeordnet.

Eine solche Anlage läuft im 15 MWe-Reaktor AVR in Jülich, mit welcher bis heute ca. 10.000 Kugeln zugegeben, 100.000 umgewälzt und ca. 10.000 entnommen worden sind. Diese Anlage hat, abgesehen von Anfangsschwierigkeiten und einigen leicht behebbaren Fehlern, im Leistungsbetrieb sich gut bewährt.

Abb. 1 zeigt einen Schnitt durch den THTR-Primärteil, in welchen die einzelnen Anlageteile der Beschickungsanlage für das 300 MWe-Kernkraftwerk zu erkennen sind:

Der Reaktorkern ist nach unten durch ein 800 mm ϕ Rohr verlängert für den Kugelabzug. Am Ausgang dieses Rohres im Beschickungsraum befinden sich zwei Vereinzeler und Schrottabscheider.

Vom Zugaberaum (links) erfolgt die Nachfüllung frischer Elemente. Diese werden aus ihren Transport- und Lagerkanistern in die Zugabeöffnungen eingegeben und laufen nach letzter Sichtkontrolle in Vorratsstrecken, d. h. Rohre in Räumen der Reaktorhalle. In Losen zu 60 Stück werden sie in den Kugelumlauf eingeschleust.

Die Umwälzung und Messung befindet sich im Beschickungsraum.

Die Förderung besteht aus der Aufspaltung des einen Umwälzstranges in 15 Förderrohre, die ebenfalls des Kerns in 3 Mittel- und 12 Randpositionen münden. Das Fördergassystem und alle beweglichen Elemente der Kugelförderung sind ebenfalls im Beschickungsraum untergebracht.

Von dort gehen die drei parallelen Stränge der Entnahme

abgebrannter Elemente über einen Zwischenkanal zum Entnahmeschleusenraum. Nach Gasdruckabsenkung werden im Entnahmeraum Elemente in verschließbare Kannen abgefüllt.

Abb. 2 stellt das Fließschema dar. Zugabe und Abzug münden in die Umwälzstrecke, die sich nach der Drucksperre in Entnahme und Förderung aufspaltet. Zur Förderung gehört ein eigener Förder- und Bremsgaskreislauf. Man bekommt durch diese Darstellung ein Bild von der Vielzahl einzelner Elemente. Diese werden Funktionsteile genannt und haben folgende Aufgaben:

Vereinzelner	bringt Kugeln aus einem Vorrat einzeln und nacheinander in ein Rohr, dient bei Stillstand der Scheibe als Kugelsperre;
Schrottabscheider	sortiert Bruchstücke, abgeplattete oder abgeriebene Kugeln aus;
Zählspule	registriert einzelne vorbeilaufende Kugeln, gibt Signal bei davorstehender Kugel: = Füllstandsanzeige;
Halteklinke	gibt bei Betätigung die vor ihr stehende Kugelsäule frei;
Dosierer	gibt bei Betätigung jeweils eine Kugel frei;
Sammler	ist eine Zusammenführung zweier Stränge, wegen Verklemmgefahr (trotz steuertechnischer Verriegelung) ausbaubar, im Betrieb unbeweglich;
Schnellschlußventil	schließt automatisch bei Druckabfall im Beschickungssystem;
Reparaturarmatur	schließt ferngesteuert von Hand, um das Reaktordrucksystem abzusperren, wenn der Ausbau eines Funktionsteils erfolgen soll;
Drucksperre	verhindert Fördergasströmungen in Richtung Meßanlage;

Höhenförderer	ist die Zusammenführung eines Kugel- und eines Gasrohres, in dem geringer Überdruck herrscht. Bis hier rollt die Kugel, ab hier wird sie pneumatisch gefördert;
Weiche	lenkt die Kugel in eine vorgewählte Bahn;
Trimmarmatur	dient zum Einstellen des Fördergas- bzw. Bremsgasdruckes;
Durchflußmessung	signalisiert, wenn eine Kugel im Förderrohr ist;
Verzögerung	ist die Zusammenführung eines Förder- und eines Gasansaugrohres. Hier wird die Austrittsgeschwindigkeit der Kugel verringert;
Abbrandmessung	stellt den Gehalt an spaltbarem Uran fest;
Unterscheidungsmessung	trennt Brenn-, Bor- und Graphitelemente voneinander.

Konstruktionsprinzipien

Das Gas in der Beschickungsanlage ist Helium von 40 ata und 260° C, das radioaktive Edelgasisotope enthält; Reaktor - Primärgas. Brennelemente, die einmal den Reaktor durchlaufen haben - im Durchschnitt werden sie sechsmal umgewälzt - strahlen. Das System ist daher nicht zugänglich, obwohl es weit vom Reaktorkern entfernt ist. Die zum Teil in 7-Sekunden-Folge bewegten Funktionsteile müssen entsprechend häufig und daher leicht gewartet bzw. repariert oder ausgetauscht werden können. Diese Forderung erfüllt man ähnlich wie bei Armaturen in aktiven Anlagen und Kreisläufen: man setzt den Antriebsteil nach außen vor eine Abschirmung. In unserem Fall wird im Wartungsfall der Funktionsteilkopf und der Abschirmstopfen mit in eine Blei-Ausbauglocke gezogen. Antrieb, Steuerung und Dichtung befinden sich vor der Abschirmdecke und sind direkt zugänglich. Man hat auf diese Weise einen Beschickungsraum, der für normale Wartungen und Störungen nicht betreten zu werden braucht. Vor den Abschirmwänden befinden sich die Steuerung der Abbrandmeßanlage, sowie Hilfs-

kreisläufe und alle Meßverstärker, auch die der Zählspulen. Die Antriebsenergie ist elektromotorisch für Schrottabscheider, Vereinzelner und Fördergebläse, pneumatisch für alle anderen beweglichen Funktionsteile und federkraftschließend für die Schnellschlußventile.

Das zweite wesentliche Konstruktionsprinzip ist die weitgehende Vereinheitlichung der Elemente, wie in Abb. 3 im Prinzip dargestellt. Hier sieht man links beginnend: Dosierer, Weiche, Drucksperre, Sammler, Zähler, Höhenförderer, Schnellschlußventil, Reparaturventil und Anpreßvorrichtung für die Sitzdichtung. Das Baukastenprinzip ist mit dem Erfolg verwirklicht worden, daß in einem Block von 2 x 1 x 0,8 m in 4 parallelen Reihen 30 Funktionsteile untergebracht sind. Da auch der Antrieb mit 2 Endstellungen vereinheitlicht wurde, sind statt einiger Mehrwegeverteiler mehrere hintereinandergeschaltete Zweiwegweichen vorhanden. Trotzdem ist letzteres sicherer, billiger und durch die Blockanordnung mit der engen Teilung nicht platzraubender.

Zugänglichkeit

Erwähnt wurde schon die Zugänglichkeit zu Funktionsteilen, Meßgebern und Steuerungen als den wartungsbedürftigen Bestandteilen der Anlage. Die Zugabestrecke bis zur Schleuse bereitet für die Zugänglichkeit keine Probleme, auch nicht für die Rohre selbst. An die Rohre und Blöcke in Umwälz-, Abzugs-, Förder- oder Entnahmestrecke kommt man heran, nachdem die Anlagen von Kugeln und Primärgas befreit und gespült sind. Da das Kugelabzugsrohr und die Bruchkammen extra abgeschirmt sind, ist der Zugang in den Beschickungsraum nach Vorbereitungszeit möglich. Läßt sich das System nicht vollständig von Kugeln befreien, so verlängert sich die Wartezeit und es sind spezielle örtliche Abschirmungsmaßnahmen zu treffen. Rohre in der Spannbetonbehälterwand und im Innern des Behälters sind nicht zugänglich. Für Funktionsteile der Entnahmestrecke gilt dasselbe wie für die Umwälzung. Für den Entnahmeraum sind bei Störfällen, die das Entfernen von Kugeln bzw. Abfüllkammen vor Betreten verhindern, Sondermaßnahmen erforderlich; allerdings nicht für verschleißbedingte Störungen. Fördergebläse und Graphitstaubfilter sind nach unten ausbaubar.

Störungsarten und Behebung

Folgende Störungsarten sind denkbar

- Hilfskreisläufe, Vorsteuerungen, Antriebsenergieversorgung, Meßwertübertragung und -verarbeitung, Programmsteuerung sind frei von direkten Einflüssen von strahlenden Kugeln oder Primärgas, leicht und schnell behebbar.

- Funktionsteilantriebe sind getrennt demontierbar, daher leicht und schnell behebbar.

- Dichtstellen an Flanschen sind nur in Ausbauräumen vorhanden (im Beschickungs- und Entnahmeraum sind alle Verbindungen geschweißt). Bei größerer Leckage muß zur Reparatur die Beschickungsanlage drucklos gemacht werden.

- Wellendichtungen der Funktionsteile können betrieblich durch Fettdruckaufgabe nachgebessert werden, unterliegen jedoch dem natürlichen Verschleiß, die Metallfaltenbälge für den Schrottabscheiderantrieb der Alterung.

- Die von Kugeln und Gas berührten Köpfe der Funktionsteile sind robust, haben großes Spiel und sind weitestgehend ausfallsicher. Ein komplettes Funktionsteil kann an einem Tag ausgetauscht werden, ausgenommen Reparaturventile, Schrottabscheider, Vereinzelner und die Schrottkanne.

- Reparaturventile, Schrottabscheider und Vereinzelner liegen an bzw. vor der Absperrgrenze. Zur Reparatur muß der Reaktor druckentlastet werden.

- Fördergasgebläse mit Motor und Staubfilter sind leicht ausbaubar konstruiert, sie können mit den abgeschirmten Ausbaugeräten für die Schrottkanne gehandhabt werden.

- Abbrand- und Unterscheidungsmeßanlage sind so aufgebaut, daß alle störungs- und verschleißbedingten Wartungen von den Ausbauräumen aus vorgenommen werden können.

- Undichtigkeiten beim Ansetzen von Schrottbehälter oder Entnahmekannen werden beim Evakuieren sofort bemerkt. Durch mehrere indirekte und eine direkte Füllstandsmessung wird Überfüllen wenig

wahrscheinlich. Der Antrieb des Transportwagens für Entnahmekannen ist mit wenigen Handgriffen auswechselbar.

- Kugelverklemmungen in Funktionsteilköpfen sind durch konstruktive Ausbildung und die hohe Zerdrückfestigkeit unwahrscheinlich. Sollte mehrfaches Bewegen des Funktionsteilkopfes ergebnislos bleiben, kann die Kugel mit ausgebaut werden. Eine entsprechend abgeschirmte Glocke ist vorhanden. Größere Staubmengen, die die Kugelrollbahn zusetzen könnten, sind erfahrungsgemäß nicht zu erwarten.

- Kugelverklemmungen im Rohr oder Block sind nur denkbar durch plötzliche Spaltung einer Kugel in zwei etwa gleich große Stücke oder durch Kugelbruchstücke, die nach Passieren des Schrottabscheiders entstanden sind. In der Praxis sind solche Fälle noch nicht beobachtet worden. Kommt es dazu, muß der Beschickungsraum begangen und das Rohrstück herausgenommen und ersetzt werden (wenn nicht äußerliche Maßnahmen helfen).

- Kugelverklemmungen in einem Förderrohr innerhalb der Betonbehälterwand oder im Behälterinneren können zum Verlust des Rohres führen.

- Rohrbrüche sind im Beschickungsraum mit Aufwand behebbar, eventuell streckenweiser Ersatz. Reißen von Blöcken, das nicht reparierbar ist, wird nicht betrachtet.

- Die Scheibe des Vereinzelners stellt die Absperrung zum Kugelhaufenkern dar und ist nicht ausbaubar, da kein Anlaß für ein schnelles Entleeren des Cores besteht. Sie ist ein Massivteil, dessen Lager ausgebaut werden kann. Bei entsprechend starkem Antrieb wäre sie in der Lage, Kugeln zu zerdrücken. Metallische Teile, die in den Kugelhaufen fallen könnten, gibt es nicht. Es sind zwei Vereinzelner für 100 % Leistung vorgesehen, so daß einer äußerstenfalls aufgegeben werden kann.

- Rohrbrüche in der Behälterwand und im Innenraum sind wegen des Einbetonierens bzw. der Druckgleichheit schwer vorstellbar. Ein Riß würde wahrscheinlich nicht stören. Schlimmstenfalls tritt der Verlust des Rohres ein.

Zuverlässigkeit - Auslegung

Der 300 MW-Reaktor ist für eine Lebensdauer von 30 Jahren ausgelegt.

Um den Brennstoff optimal zu nutzen, ist zu jedem Zeitpunkt die Zugabemenge und -sorte von Elementen und die Verteilung der die Meßanlage passierenden Kugeln auf die einzelnen Core-Positionen nach einem Programm vorzunehmen. Da der Zustand des Kugelhaufens ständig verfolgt wird und die tägliche Nachfüll- und Entnahmemenge klein im Vergleich zu der im Kern vorhandenen Menge an Elementen ist, ca. 1 : 1000, kann im Störfall über längere Zeit auf den Betrieb der Beschickungsanlage verzichtet werden. Der Reaktor kann etwa 40 Tage lang mit Vollast betrieben werden, wobei die eingebaute Überschußreaktivität zum Überfahren der Xenonvergiftung nach Lastwechsel teilweise aufgebraucht wird.

Die integrierte Ausfallzeit der Beschickungsanlage innerhalb von 30 Jahren soll daher in der Größenordnung von 40 Tagen liegen, vorausgesetzt, daß Einzelereignisse wesentlich darunter liegen.

Für einen optimalen Betrieb sollte die Beschickungsanlage ständig laufen, so lange der Reaktor in Betrieb ist. Die Leistungsauslegung aller Stränge der Anlage sieht vor, die für einen Reaktorbetriebstag notwendigen Operationen in einer 8-Stunden-Schicht ausführen zu können. Diese Diskontinuität fällt nicht ins Gewicht. Somit hat die Anlage eine Leistungsreserve von 200 %. Die täglich 16 betriebsfreien Stunden werden zum Teil für die Wartung benutzt. Ferner sind in den planmäßigen Abschaltpausen im 4-Jahres-Zyklus Wartungsarbeiten auszuführen.

Für die Funktionsteile sind bestimmte störungsfreie Betriebszeiten vorgeschrieben:

Gesamtanlage	30 Jahre
ausgenommen: Verschleißteile, die routinemäßig auswechselbar sind	1 Jahr
Der Belastungsgrad wird wie folgt berücksichtigt:	
Funktionsteile	$2 \cdot 10^6$ Kugeln
Schleusenarmatur	10^4 Betätigungen
Schnellschlußventile	$5 \cdot 10^2$ Betätigungen
Verschleißteile, die nicht routinemäßig, d. h. ohne Einfluß auf den Reaktorbetrieb, auswechselbar sind	4 Jahre

Belastungsgrad:

Reparaturarmaturen	$2 \cdot 10^3$ Betätigungen
Lager und Balgdichtung von Vereinzelner und Schrottabscheider	$8 \cdot 10^6$ Kugeln

Redundanzbetrachtung

Die Mehrfachanordnung einzelner Stränge nach Abb. 2 bedeutet nicht in allen Fällen echte Redundanz:

- Der zweite Strang in der Zugabe vor der Weiche wird während der Anfangsphase vornehmlich Borkugeln zur schnellen Korrektur von Berechnungsunsicherheiten bei der örtlichen Leistungsverteilung enthalten. Nach genauerer Kenntnis des Core-Verhaltens und Beendigung der Einlaufphase ist der zweite Strang eine echte Verdoppelung.
- Die drei parallelen Stränge hinter der Zugabeschleuse werden nach dem Rechnerprogramm für die Neubeschickung des kommenden Tages gefüllt, in den ersten drei Jahren mit max. 865 und danach mit 711 Elementen. Jeder Strang kann 300 Kugeln aufnehmen. (Auch die Pufferstrecken vor der Zugabeschleuse haben dieses Fassungsvermögen.) Fällt hiervon ein Strang aus, so kann die restliche Tagesfüllung nicht auf Vorrat eingeschleust werden. Dies bedeutet keine Einbuße an Verfügbarkeit der Zugabestrecke, sondern betriebliche Maßnahmen. Eine Reparatur würde man erst bei Gelegenheit vornehmen. Auch bei zwei ausgefallenen Strecken ist, wenn auch mit erhöhtem Aufwand, z. B. Mehrschichtbetrieb, die Zugabestrecke noch voll verfügbar. Die Schleusenzeit für 60 Kugeln ist ca. 20 min. In der nachfolgenden Analyse wird die Zugabestrecke in ihren drei Zonen als 1-von-2, 1-von-1 und 1-von-3 Schaltung betrachtet.
- Echt doppelt vorhanden sind die zwei Schrottabscheider / Vereinzelnereinheiten der Abzugstrecke.
- Für eine zweckmäßige Aufteilung des Cores in zwei Zonen sind wegen der Sehnittkegelgrenzen 3 Rohre innen und 15 am Rand angeordnet.

Der Verlust eines Rohres verschiebt örtlich diese Grenze und ergibt eine ungleiche Füllhöhe. Dieser Umstand kann in der Programmrechnung berücksichtigt werden und beeinflußt nicht den Reaktorbetrieb. Fällt ein weiteres Rohr an einer nicht benachbarten Stelle aus, gilt dasselbe. Bei 15 Rohren ist die Wahrscheinlichkeit, daß zwei Rohre nebeneinander liegen, noch genügend klein. Erst bei einem dritten Rohrausfall ist damit zu rechnen. Es würde dann eine geringe Beeinflussung des Reaktorbetriebes hinsichtlich der Wirtschaftlichkeit auftreten. Es können somit zwei Rohre als redundant angesehen werden. Obwohl ein weiterer Betrieb mit drei und mehr ausgefallenen Rohren grundsätzlich möglich ist, wird in der nachfolgenden Analyse bereits "Ausfall" angesetzt.

- Für das Ausbringen von abgebrannten Elementen aus dem Beschickungskreislauf und das gleichzeitige Abfüllen solcher Kugeln in Entnahmekannen braucht man zwei Stränge, da die Pufferstrecke die Schleuse selbst ist. Der dritte Strang in der Entnahme erleichtert durch zyklisches Vertauschen den Betrieb. Fällt er aus, kann die Abfüllung einer Tagesmenge in die Entnahmekanne unter Umständen nicht mehr in einer Schicht erfolgen. Die Reparatur erfolgt bei Gelegenheit. Ein Strang gilt als redundant. Fällt ein weiterer aus, so muß der Beschickungsbetrieb für die Dauer der Kannenabfüllung, d. h. ca. 50 min. täglich unterbrochen werden. In der nachfolgenden Analyse wird daher die Entnahmestrecke pessimistisch als 2-von-3 - Schaltung angesehen.

Ausfallgesetz

Unter den verschiedenen Gesetzmäßigkeiten für die zeitliche Abhängigkeit der Ausfallrate ist für die Elemente der Beschickungsanlage die der zeitlichen Konstanz anzuwenden. Von der "Badewannenkurve" kann der vordere Teil der Frühausfälle abgeschnitten werden, da eine sehr eingehende Betriebserprobung der [illegible] vorangeht, [illegible]

mit dem Ziel, das Gerät in einen solchen Zustand zu versetzen, daß es ein nächstes Intervall mit gleicher Zuverlässigkeit übersteht wie das vorhergehende, bis max. 30 Jahre.

Die Zuverlässigkeit ist also an die Wartungs- oder Inspektionsintervalle gebunden. (Im folgenden wird nur noch von "Intervallen" gesprochen.)

Die Konstruktion der Teile und das dazugehörige Wartungskonzept wurde so gewählt, daß bei Einhalten der geforderten Lebensdauer = störungsfreie Zeiten die Ausfallrate der Beschickungsanlage null ist, weil die Wartungsarbeiten entweder bei laufendem Betrieb oder in planmäßigen Stillstandszeiten durchgeführt werden können. Die Verfügbarkeit der Beschickungsanlage wäre dann gleich 1,0.

Neben den Größen Intervall J und Reparaturzeit R wird für die Ausfallrate eines Teils die Häufigkeit H gebraucht:

$$A = H \frac{R}{J}$$

H wird definiert als Wahrscheinlichkeit des Eintretens eines Störereignisses im Intervall J. H und J müssen also immer zusammen gesehen werden. R schließt die Zeit vom Eintreten des Ereignisses bis zur Wiederinbetriebnahme nach Ausbesserung und Prüfung ein.

Die A-Werte verschiedener Teile, auch bei unterschiedlichen Intervallen, sind vergleichbar.

Bei irreparablen Störungen wird R = 15 Jahre, denn das Auftreten innerhalb des 30-Jahre-Intervalls findet im Mittel nach Ablauf der halben Zeit statt.

Ausgangswerte

In Tabelle 6 sind die benutzten Werte für die Ausfallrate im dazugehörigen Intervall genannt. In der Literatur sind erwartungsgemäß statistische Zuverlässigkeitsangaben für neuartige Konstruktionen nicht enthalten. Es werden daher, soweit möglich, Erfahrungen ähnlicher Elemente aus der AVR-Beschickungsanlage verwendet. Die neuartigen Funktionsteile werden einzeln und in Zusammenschaltung als Prototypen getestet. Die Teile der Reaktor-Beschickungsanlage werden einem mehrmonatigen Funktionstest unterzogen, so daß eine Bestätigung oder Berichtigung der Werte aus Tabelle 6 nach Inbetriebnahme des Reaktors teilweise möglich ist.

Für die Analyse wird im Grundsatz davon ausgegangen, daß bei auslegungsgemäßer Beanspruchung von 10 Teilen eines im Intervall ausfällt: 1a, 4a, 5a, 7a. Bei geringerer Beanspruchung (Belastungsfaktor) wird anteilig bis auf 20 % dieses Wertes zurückgegangen. Gebläse und Staubfilter können in der Funktion versagen durch Motor- oder Lagerschaden bzw. Belegung mit Fremdkörpern (außer Graphitstaub) und Feuchte in Störfällen: 12a, 13a. Über diese Arten von mechanischem Versagen = Störungsart a hinaus wird angenommen, daß unzulässige Gasleckagen an Flansch oder Welle auftreten, deren Behebung einen Ausbau erfordert: 1b - 7b, 12b, 13b, 14b; und daß im Funktionsteilkopf Kugeln verklemmen: 1c - 8c. Pessimistischerweise wird dies trotz gegenteiliger Erfahrungen mit guter Statistik auch für Rohre, Blöcke und als Überfüllung von Kannen betrachtet. Steuer- und Vorsteuerungen werden mit Ausnahme für die Meßanlage in der Auswirkung als zentral beeinflussend angenommen und Störungen, die bis zu zwei Tage Reparaturzeit erfordern, für denkbar gehalten: 1d - 12d. Bei Armaturen läßt bekanntlich die Sitzdichtigkeit nach. Dies soll trotz Wartung berücksichtigt werden: 3e - 5e. Meßgeber sind leicht austauschbar angeordnet und werden nicht betrachtet, da ihre Reparaturzeit unter einem Tag liegt. Störungen an den Venturi-Düsen des Fördergassystems sind kaum vorstellbar. Deshalb ist kein Routineausbau geplant: 3f. In der Analyse werden Komplikationen beim Austausch der Meßgeber der Kugelmeßanlagen berücksichtigt: 10f. Hilfskreisläufe liegen mit ihren wartungsbedürftigen Elementen grundsätzlich außerhalb des Beschickungsraumes, sind leicht zugänglich und in Stunden zu reparieren. Auch hier werden Komplikationen bei der Ausbesserung betrachtet: 4g, 10g, 12g, 13g.

Grundsätzlich sind nur Störungen in der Tabelle aufgenommen, deren Behebung mindestens einen Tag dauert, da sonst die Verfügbarkeit der Beschickungsanlage nicht beeinflußt wird.

Die Werte von H und J der Störungsarten b bis f werden in Relation zu denen von a gebracht. Daneben werden Relationen der "störanfälligen" Teile 1 bis 16 betrachtet. Durch dieses Kreuzschema bleibt für das Ermessen einzelner Annahmen wenig Spielraum. Man kann also davon ausgehen, daß die Einsatzausfallhäufigkeiten vertretbar gesichert sind, sofern die Basis jedes zehnte Funktionsteil fällt einmal pro Intervall aus, anerkannt wird.

Auswertung

Diese erfolgt abschnittweise für die fünf Abschnitte der Anlage = Zugabe, Abzug, Umwälzung, Förderung, Entnahme (siehe Abb. 4 und 5, Tabellen 7 bis 11).

Zunächst wird das Fließschema des Abschnitts und sämtliche hierzu enthaltenen störungsverursachenden Teile betrachtet. Bei bestimmten Teilen wird der Belastungsgrad festgestellt. Für die Reparaturzeit ist die Zugänglichkeit entscheidend. Der Raum, von dem aus die Behebung erfolgt, ist angegeben; wobei bedeutet:

AR	Ausbauraum
BR	Beschickungsraum
EAR	Entnahmeschleuse - Ausbauraum
ER	Entnahmeraum
ESR	Entnahme - Schleusenraum
Halle	Reaktorhalle - Räume (Kontrollbereich)
SAR	Steuerarmaturen - Ausbauraum
SBB	Spannbetonbehälter (unzugänglich)
ZR	Zugaberaum
ZSR	Zugabeschleusenraum

Die Reparaturzeit umfaßt definitionsgemäß auch Warte- und Vorbereitungszeiten.

Es wird ein Ersatz- Schaltbild des Abschnitts gezeichnet = Abb. 4 und 5. Hiernach kann - bei Berücksichtigung der echten Redundanzen, siehe oben - die Zuverlässigkeit bzw. Ausfallrate des Abschnitts aus der der einzelnen Teile bestimmt werden:

Abschnitt Ausfall	Rechnerische Verknüpfung der Einzel-Ausfallraten	Ausfallrate x 10^6	
Zugabe	siehe Abb. 5		
1 Luftstrang defekt	$2 \cdot \sum(① - ⑤) + ⑮$	142	
1 Gasstrang defekt	$3 \cdot (⑫ + ⑬ + ⑰)$	504	
2 Gasstränge defekt	$3 \cdot (⑫ + ⑬ + ⑰)^2 + ① + ⑭$	137	
Zugabe ausgefallen	$\sum(⑥ - ⑩) + ⑯ + ⑱ + ⑲ + 2 \cdot ⑭$		1257
Abzug	siehe Abb. 4		
1 Strang defekt	$2 \cdot (① + ② + ③ + ④)$	1802	
Abzug ausgefallen	$\sum(① - ④)^2 + \sum(⑤ - ⑫)$		931
Umwälzung	siehe Abb. 4		
Umwälzung ausgefallen	$\sum(① - ⑦)$		1668
Förderung	siehe Abb. 4		
1 Strang defekt	$15 \cdot (⑥ + ⑦ + ⑧ + ⑨ + ⑱ + ⑰) + 2 \cdot ⑤$	74580	
2 Stränge defekt	$105 \cdot (⑥ + ⑦ + ⑧ + ⑨ + ⑰ + ⑱)^2 + 2 \cdot ⑤$	3339	
Förderung ausgefallen	$\sum(① - ④) + \sum(⑩ - ⑫) + (\ldots + 12 \cdot ⑤$		1976
Entnahme	siehe Abb. 5		
1 Strang defekt	$3 \cdot \sum(④ - ⑨) + ③ + ⑬$	1543	
Entnahme ausgefallen	$3 \cdot (\sum(④ - ⑨) + ⑬)^2 + ① + ② + \sum(⑩ - ⑫)$		426

Ergebnis

Erwartungsgemäß ist die Ausfallrate eines Stranges gleich oder größer der des Abschnitts. Bei der Zugabe dagegen ist es wahrscheinlicher, daß sie im ganzen ausfällt, als daß ein Strang unbrauchbar wird. Das zeigt, daß hier die Mehrfachanordnung der parallelen Stränge primär aus Gründen der Betriebsvereinfachung und nicht wegen erhöhter Zuverlässigkeit vorgesehen ist.

Stellt man die Ausfallraten der fünf Abschnitte gegenüber:

Zugabe	$1257 \cdot 10^{-6}$
Abzug	$931 \cdot 10^{-6}$
Umwälzung	$1668 \cdot 10^{-6}$
Förderung	$1976 \cdot 10^{-6}$
Entnahme	$426 \cdot 10^{-6}$
	$6258 \cdot 10^{-6}$

so sieht man, daß eine annähernd gleichmäßige Zuverlässigkeit erreicht worden ist. Die Annahme irreparabler Schäden bei Förderung und Abzug wirkt sich im Ergebnis kaum aus. Die relativ hohe Rate bei der Förderung ist bedingt durch die hohe Zahl (22) zentral beeinflussender Störquellen. Die Ausfallrate der Umwälzung ist bedingt durch den hohen Belastungsgrad weniger Funktionsteile, durch die aber jede einzelne Kugel läuft.

In 30 Jahren bedeutet die Gesamtausfallrate von $6{,}258 \cdot 10^{-3}$

$$0{,}19 \text{ Jahre} = 68 \text{ Tage}$$ Ausfall der Beschickungsanlage.

Das Einzelteil mit höchster Rate für die Gesamtanlage ist die Abbrandmeßanlage mit $0{,}512 \cdot 10^{-3}$, gefolgt von Schleusenventilen der Zugabe mit $0{,}378 \cdot 10^{-3}$ und Defekten der Umwälzung mit $0{,}353 \cdot 10^{-3}$.

Da erwähnt wurde, daß die Beschickungsanlage ca. 40 Tage stillstehen kann, ohne grössere Einbuße an Verfügbarkeit für den Reaktor zu verursachen, und da die Wahrscheinlichkeit genügend gering ist, daß die Ausfallzeiten der Anlage unmittelbar aufeinander

folgen, sondern sich auslegungsgemäß etwa gleichmäßig über 30 Jahre verteilen werden, ist die ermittelte Ausfallrate klein genug.

Die Verfügbarkeit der Beschickungsanlage beträgt damit 99,37 %.

Alternativen

Zwei Alternativanordnungen wurden untersucht:

a) Echte Verdoppelung der Abschnitte Abzug, Umwälzung und Förderung.
Die Ausfallraten sind in diesem Fall:

Zugabe	$1257 \cdot 10^{-6}$
Abzug	$3 \cdot 10^{-6}$
Umwälzung	$3 \cdot 10^{-6}$
Förderung	$4 \cdot 10^{-6}$
Entnahme	$426 \cdot 10^{-6}$
	$1693 \cdot 10^{-6}$

Gesamtausfallzeit in 30 Jahren: 19 Tage
Verfügbarkeit: 99,80 %

Hier zeigt sich, daß es unzweckmäßig wäre, Entnahme und Zugabe unverändert zu lassen. Es bietet sich daher die Lösung einer vollständigen Anordnung zweier getrennter, je für 100 % Leistung ausgelegter Anlagen, wie es die ursprüngliche Konzeption war, an.

b) Echte Verdoppelung der gesamten Beschickungsanlage, einschließlich Steuerungen, Hilfskreisläufe, gemeinsame Entnahmestation.
Die Ausfallraten sind in diesem Fall:

Zugabe	$1 \cdot 10^{-6}$
Abzug	$3 \cdot 10^{-6}$
Umwälzung	$3 \cdot 10^{-6}$
Förderung	$4 \cdot 10^{-6}$
Entnahme	$72 \cdot 10^{-6}$
	$83 \cdot 10^{-6}$

Gesamtausfallzeit in 30 Jahren: 0,9 Tage

Verfügbarkeit: >99,99 %

Ausgeführt wird für den 300 MWe - Reaktor die in den Anlagen gezeigte Anordnung, da ein Übergang zur Alternative b einen unverhältnismäßig großen Kostenaufwand, vor allem wegen des Raumbedarfes zweier völlig unabhängiger Anlagen, verursachen würde.

Literatur

U. Hennings — Bewertung von Auswahlschaltungen
Atomwirtschaft, März 1963

U. Hennings — Remote Handling System for Core Elements of a Pebble Bed Reactor
Nuclear Applications (ANS), Oct. 1969

U. Cleve, H. Handel, U. Scholz — Unload Fuelling of Pebble Bed High Temperature Reactors
Symposium on Refuelling Gas-cooled Reactors, Dec. 1968, London

W. Hofmann — Zuverlässigkeit von Meß-, Steuer-, Regel- und Sicherheitssystemen
Karl Thiemig Verlag, München, 1968

H. Gieseler — Ein Vergleich der Zuverlässigkeit von Reaktorsicherheitssystemen
Vorläufiger Bericht des Institutes für Meß- und Regelungstechnik der TH München, Juni 1969

J. Ehrenteich, H. Maurer — Reliability Considerations for Electro-mechanical and Hydraulic Control Rod Drive Systems
Ispra, Juni 1968

Tabelle 6

Störungshäufigkeit h
in
Intervall J

	Teil, Anlage	Störungsart	mechanische Funktionsstörungen, Verschleiß	größere Undichtigkeit nach außen (unabhängig von a)	Kugelverklemmung, Rohrbruch	Steuer- bzw. Vorsteuereinrichtung defekt >1d	ungenügende Sitzdichtigkeit (unabhängig von a)	Meßgeber defekt >1d	Hilfskreislaufe gestört >1d
			a	b	c	d	e	f	g
1	Weiche, Dosierer, Drucksperre einschl. Antrieb	H J	0,1* 1	0,1* 4	0,05* 30	0,05 4	-	-	-
2	Zähler, Sammler, Förderer einschl. Abschlußflansch	H J	0,02 1	0,01 4	0,02 30	-	-	-	-
3	Gasarmatur (Trimmventil) einschl. Antrieb	H J	0,05 1	0,05 4	-	0,05 4	0,02 4	0,02 30	-
	Schleusenventil einschl. Antrieb	H J	0,1* 1	0,1* 4	0,02 30	0,05 4	0,01 1	-	0,025 4
5	Reparaturventil einschl. Antrieb	H J	0,1* 4	0,02 4	0,02 30	0,05 4	0,01 4	-	-
6	Schnellschlußventil einschl. Antrieb	H J	0,001 1	0,02 4	0,02 30	0,05 4	-	-	-
7	Antrieb Schrottabscheider	H J	0,1 1	0,02 4	-	0,05 4	-	-	-
8	Funktionsteil Schrottabscheider, Vereinzelnerlager	H J	0,05 30	-	0,02 30	-	-	-	-
9	Schrottkanne	H J	-	-	0,001 30	-	-	-	-
10	Abbrand- und Unterscheidungsmeßanlage	H J	-	-	0,004 30	0,1 4	-	0,4 4	0,1 4
11	Kassenentnahme	H J	0,01 4	-	0,002 30	0,05 4	-	-	-
12	Gebläse einschl. Antrieb	H J	0,1 4	0,01 4	-	0,05 4	-	-	0,05 4
13	Staubfilter	H J	0,01 4	0,01 4	-	-	-	-	0,01 4
14	Gasbehälter	H J	-	0,01 4	-	-	-	-	-
15	Kugelrohrau, Blöcke im Beschickungsraum	H J	-	-	0,001** 30	-	-	-	-
16	Gasrohre, Kugelrohre im SKD und Reaktor (druckl.)	H J	-	-	0,0005** 30	-	-	-	-

* abhängig von Belastungsfaktor

** pro m Länge

Tabelle 7

ZUGABE
(Supply line)

	Teil part	Belastung load factor	Störung failure	Häufigkeit frequency	Intervall J (Jahre) interval J (years)	Zugang von (Raum) access from (room)	Reparaturdauer (Tage) repair duration (days)	Einzelausfallrate x 10^6 individual failure rate x 10^6	Ausfallrate x 10^6 failure rate x 10^6
1	2 Vereinzelner 2 singulizer		a o	0,1 0,05	1 30	ZR* "	≤ 1 1	0 5	5
2	2 Zähler 2 counter		a	0,02	1	"	≤ 1	0	0
3	2 Halteklinken 2 stopper		a	0,1	1	"	≤ 1	0	0
4	2 Zähler 2 counter		a	0,02	1	"	≤ 1	0	0
5	2 Dosierer 2 timing device	0,2	a o	0,02 0,02	1 30	ZSR* "	1 1	56 2	58
6	Zusammenführung connecting joint		o	0,02	30	"	10	20	20
7	Schleusenventil air/gas lock valves	1,0	a b c e	0,1 0,1 0,02 0,01	1 4 30 1	" " " "	1 1 1 1	278 70 2 28	378
8	Zähler counter		a b c	0,02 0,01 0,02	1 4 30	" " "	1 1 1	56 7 2	65
9	Dosierer timing device	0,3	a b c	0,03 0,03 0,02	1 4 30	" " "	1 1 1	84 21 2	107
10	Schleusenventil air/gas lock valve		a b c e	0,1 0,1 0,02 0,01	1 4 30 1	" " " "	1 1 1 1	278 70 2 28	378

	Teil part	Belastung load factor	Störung failure	Häufigkeit frequency	Intervall J (Jahre) interval J (years)	Zugang von (Raum) access from (room)	Reparaturdauer (Tage) repair duration (days)	Einzelausfallrate x 10^6 individual failure rate x 10^6	Ausfallrate x 10^6 failure rate x 10^6
11	2 Weichen 2 switchs		a b c	0,02 0,02 0,02	1 4 30	ZSR* " "	1 1 1	56 14 2	72
12	3 Zähler 3 counter		a b c	0,02 0,01 0,02	1 4 30	" " "	1 1 1	56 7 3	66
13	3 Dosierer 3 timing devices	0,1	a b c	0,02 0,02 0,02	1 4 30	AR* " "	1 1 1	56 14 2	72
14	3 Sammler 3 collector		a b c	0,02 0,01 0,02	1 4 30	" " "	1 1 1	56 7 2	65
15	2 Rohre 5m 2 Rohre 20 m 2 tubes 5m 2 tubes 20 m		c c	0,005 0,02	30 30	ZR Halle	3 3	2 6	8
16	1 Rohr 2 m 1 Rohr 1 m 1 tube 2 m 1 tube 1 m		c c	0,002 0,001	30 30	ZSR "	3 8	1 1	2
17	3 Rohre 18 m 3 tubes 18 m		c	0,018	30	BR	20	30	30
18	Vorsteuerung part drive control		d	0,05	4	SAR*	2	70	70
19	Schleusenkreislauf air/gas lock circuit		g	0,025	4	RR*	2	55	55
	siehe Seite see page	15 16							

Tabelle 8

A B Z U G
(Extraction)

	Teil part	Belastung load factor	Störung failure	Häufigkeit frequency	Intervall J (Jahre) interval J (years)	Zugang von (Raum) access from (room)	Reparaturdauer (Tage) repair duration (days)	Einzelausfallrate x 10^{-6} individual failure rate x 10^{-6}	Ausfallrate x 10^{-6} failure rate x 10^{-6}
1	Vereinzelnerscheibe Singulizer disc		c	0,001	30	BR*	irrep	500	500
2	Schrottabscheider, Vereinzelnerlager damaged sphere separator		a c	0,05 0,02	30 30	BR "	10 30	47 56	103
3	Antrieb Schrottabscheider separator drive		a b	0,1 0,02	1 4	AR* "	1 1	278 14	292
4	Schrottkanne damaged sphere container		c	0,001	30	AR	60	6	6
5	Zusammenführung connecting joint		c	0,02	30	BR	60	112	112
6	Reparaturventil repair valve		a b c e	0,02 0,02 0,02 0,01	4 4 30 4	AR " " "	6 6 6 6	83 83 11 41	218
7	Schnellschlußventil quick acting valve		a b c	0,001 0,02 0,02	1 4 30	AR " "	1 1 1	3 14 2	19
8	Zähler counter		a b e	0,02 0,01 0,02	1 4 30	AR " "	1 1 1	56 7 2	65

Tabelle 8 - 2 -

	Teil part	Belastung load factor	Störung failure	Häufigkeit frequency	Intervall J (Jahre) interval J (years)	Zugang von (Raum) access from (room)	Reparaturdauer (Tage) repair duration (days)	Einzelausfallrate x 10^6 individual failure rate x 10^6	Ausfallrate x 10^6 failure rate x 10^6
9	Dosierer timing device	1,0	a b c	0,1 0,1 0,05	1 4 30	AR " "	1 1 1	278 70 5	353
10	Sammler collector		a b c	0,02 0,01 0,02	1 4 30	AR " "	1 1 1	56 7 2	65
11	Rohre 10m tubes 10m		c	0,01	30	BR	30	28	28
12	Vorsteuerung part drive control		d	0,05	4	SAR*	.2	70	70

* siehe Seite 13
see page 16

Tabelle 9

U M W Ä L Z U N G

(Circulating line)

	Teil part	Belastung load factor	Störung failure	Häufigkeit frequency	Intervall J (Jahre) interval J (years)	Zugang von (Raum) access from (room)	Reparaturdauer (Tage) repair duration (days)	Einzelausfallrate x 10^6 individual failure rate x 10^6	Ausfallrate x 10^6 failure rate x 10^6
1	Sammler collector	-	a b c	0,02 0,01 0,02	1 4 30	AR* " "	1 1 1	56 7 2	65
2	Zähler counter	-	a b c	0,02 0,01 0,02	1 4 30	AR* " "	1 1 1	56 7 2	65
3	Dosierer timing device	1,0	a b c	0,1 0,1 0,05	1 4 30	AR* " "	1 1 1	278 70 5	353
4	Abbrand- und Unterscheidungsmeßanlage sphere measurement	1,0	c d f g	0,004 0,1 0,4 0,1	30 4 4 4	BR* AR AR AR	60 1 1 2	24 70 278 140	512
5	Zähler counter	-	a b c	0,02 0,01 0,02	1 4 30	AR " "	1 1 1	56 7 2	65
6	Drucksperre, Dosierer pressure lock	1,0	a b c	0,1 0,1 0,05	1 4 30	AR " "	1 1 1	278 70 5	353
7	Weiche switch	0,5	a b c	0,05 0,05 0,025	1 4 30	AR " "	1 1 1	139 35 3	177
8	Rohr 3 m (Rest 4 c) tube 3 m (rest 4 c)	-	c	0,003	30	BR	30	8	8
9	Vorsteuerung PT, part drive control	-	d	0,05	4	BAR*	2	70	70
	*siehe Seite see page 16	13							

Tabelle 10

FÖRDERUNG

(Fuelling line)

	Teil part	Belastung load factor	Störung failure	Häufigkeit frequency	Intervall J (Jahre) interval J (years)	Zugang von (Raum) access from (room)	Reparaturdauer (Tage) repair duration (days)	Einzelausfallrate x 10^6 individual failure rate x 10^6	Ausfallrate x 10^6 failure rate x 10^6
1	Weiche switch	0,5	a b c	0,05 0,05 0,025	1 4 30	AR* " " " "	1 1 1	139 35 2	176
2	Zähler counter		a b c	0,02 0,01 0,02	1 4 30	" " " " " "	1 1 1	56 7 2	65
3	Dosierer timing device	1,0	a b c	0,1 0,1 0,05	1 4 30	" " " " " "	1 1 1	278 70 5	353
4	Weiche switch	0,4	a b c	0,04 0,04 0,02	1 4 30	" " " " " "	1 1 1	112 28 2	142
5	13 Weichen 13 switchs	0,2	a b c	0,02 0,01 0,02	1 4 30	" " " " " "	1 1 1	56 7 2	65
6	15 Förderer mit Zähler 15 elevators plus counters		a b c	0,02 0,01 0,02	1 4 30	" " " " " "	1 1 1	56 7 2	65
7	Schnellschluß- ventile 15 quick ac- ting valves		a b c	0,02 0,05 0,02	1 30 30	" " " " " "	1 1 1	56 5 2	63
8	15 Reparatur- ventile 15 repair valves		a b c e	0,02 0,02 0,02 0,01	4 4 30 4	" " " " " " " "	6 6 6 6	84 84 12 42	222
9	15 Gasarmatu- ren 15 gas valves		a b e f	0,05 0,05 0,02 0,02	1 4 4 30	" " " " " " " "	1 1 1 30	139 35 14 56	244

	Teil part	Belastung load factor	Störung failure	Häufigkeit frequency	Intervall J (Jahre) interval J (years)	Zugang von (Raum) access from (room)	Reparaturdauer (Tage) repair duration (days)	Einzelausfallrate x 10^6 individual failure rate x 10^6	Ausfallrate x 10^6 failure rate x 10^6
10	Gebläse gas circulator		a b g	0,1 0,01 0,05	4 4 4	AR* " "	3 2 2	210 14 70	294
11	Staubfilter dust filter		a b g	0,01 0,01 0,01	4 4 4	" " "	2 2 2	14 14 14	42
12	Gasbehälter gas container		b	0,01	4	"	2	14	14
13	5 Gasarmaturen 5 gas valves		a b e f	0,05 0,05 0,02 0,02	1 4 4 30	" " " BR	1 1 1 30	139 35 14 56	244
14	5 Schnell-schlußventile 5 quick acting valves		a b c	0,02 0,05 0,02	1 30 30	AR " "	1 1 1	56 5 2	63
15	5 Reparatur-ventile 5 repair valves		a b c e	0,02 0,02 0,02 0,01	4 4 30 4	" " " "	6 6 6 6	84 84 12 42	222
16	1 Rohr + 2 Blöcke 3m 1 tube + 2 blocks 3m		c	0,003	30	BR	30	9	9
17	15 Rohre je 5m im BR je 20m im SEB* 15 tubes 5m each in BR, 20 m each in SEB		c c	0,005 0,01	30 30	" SEB*	30 irrep.	15 5000	5015

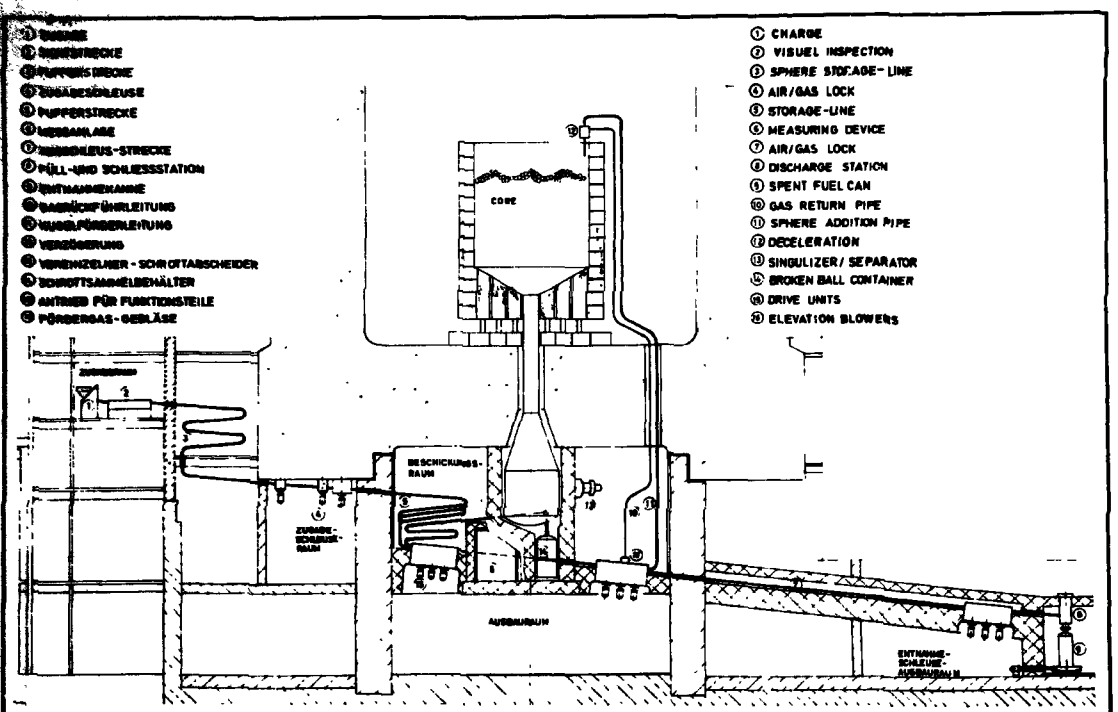
	Teil part	Belastung load factor	Störung failure	Häufigkeit frequency	Intervall J (Jahre) interval J (years)	Zugang von (Raum) access from (room)	Reparaturdauer (Tage) repair duration (days)	Einzelausfallrate $\times 10^6$ individual failure rate $\times 10^6$	Ausfallrate $\times 10^6$ failure rate $\times 10^6$
18	15 Gasrohre 7 m 15 gas tubes 7 m		c	0,004	30	BR	30	21	21
19	1 Gasrohr 8 m 1 gas tube 8m		c	0,004	30	"	30	24	24
20	5 Gasrohre 8m 5 gas tubes 8m		c	0,004	30	"	30	24	24
21	Vorsteuerung part drive control		d	0,05	4	SAR	2	70	70
	*siehe Seite see page 16	13							

Tabelle 11

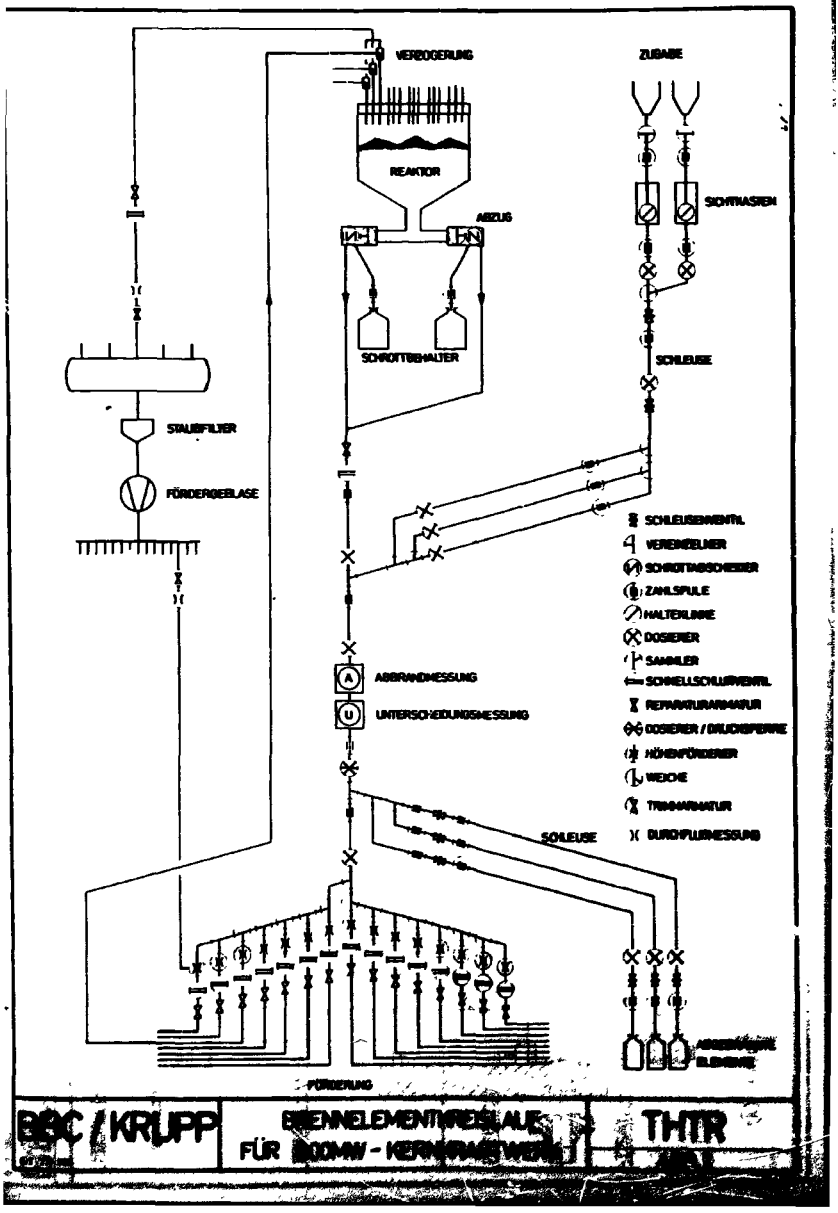
ENTNAHME
(Discharge line)

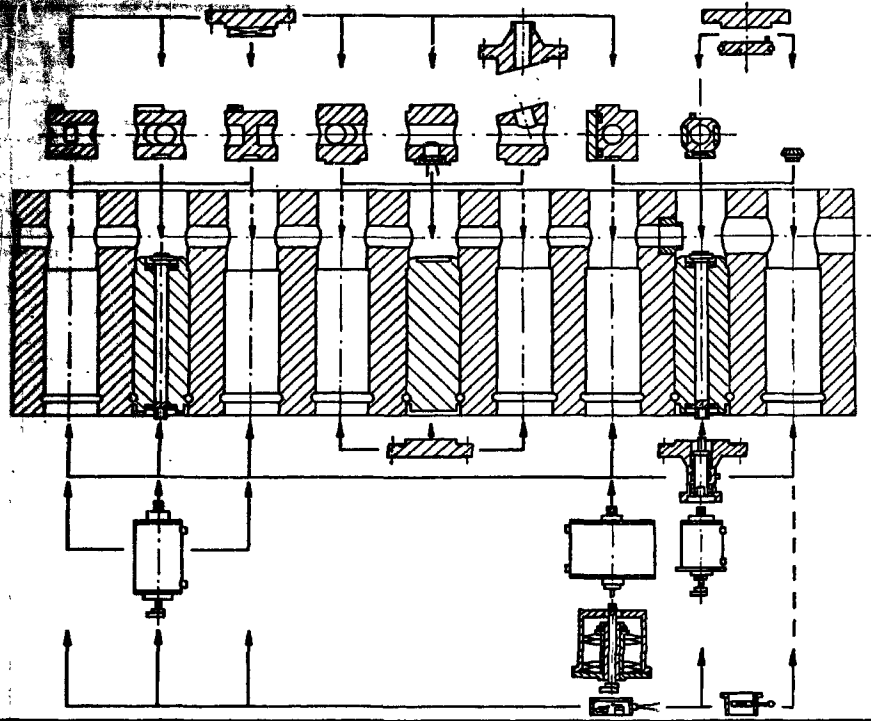
	Teil part	Belastung load factor	Störung failure	Häufigkeit frequency	Intervall J (Jahre) interval J (years)	Zugang von (Raum) access from (room)	Reparaturdauer (Tage) repair duration (days)	Einzelausfallrate $\times 10^6$ individual failure rate $\times 10^6$	Ausfallrate $\times 10^6$ failure rate $\times 10^6$
1	Weiche switch	0,5	a b c	0,05 0,05 0,025	1 4 30	AR* " "	1 1 1	139 35 3	177
2	Weiche switch		a b c	0,02 0,02 0,02	1 4 30	AR* " "	1 1 1	56 14 2	72
3	Weiche switch		a b c	0,02 0,02 0,02	1 4 30	" " "	1 1 1	56 14 2	72
4	3 Zähler 3 counter		a b c	0,02 0,01 0,02	1 4 30	AR* " "	1 1 1	56 7 2	65
5	3 Schleusen- ventile 3 air/gas lock valves	0,2	a b c e	0,02 0,02 0,02 0,01	1 4 30 1	" " " "	1 1 1 1	56 14 2 28	100
6	3 Zähler 3 counter		a b c	0,02 0,01 0,02	1 4 30	AR* " "	1 1 1	56 7 2	65
7	3 Dosierer 3 timing de- vices	0,1	a b c	0,02 0,02 0,02	1 4 30	HAR* " "	1 1 1	56 14 2	72
8	3 Schleusen- ventile 3 air/gas lock valves	0,2	a b c e	0,02 0,02 0,02 0,01	1 4 30 1	HAR* " " "	1 1 1 1	56 14 2 28	100
9	3 Zähler 3 counter		a b c	0,02 0,01 0,02	1 4 30	HAR* " "	1 1 1	56 7 2	65
10	Kannenentnahme spent fuel fil- ling station		a c	0,01 0,002	4 30	HR* "	10 10	70 2	72

	Teil part	Belastung load factor	Störung failure	Häufigkeit frequency	Intervall J (Jahre) interval J (years)	Zugang von (Raum) access from (room)	Reparaturdauer (Tage) repair duration (days)	Einzelausfallrate x 10^6 individual failure rate x 10^6	Ausfallrate x 10^6 failure rate x 10^6
11	Schleusen-kreislauf air/gas lock circuit		g	0,025	4	SAR*	2	35	35
12	Vorsteuerung der FT part drive control		d	0,05	4	SAR	2	70	70
13	Rohre und Blöcke 3 x 5m 3 x20m tubes and blocks 3 x 5m 3 x20m		o o	0,005 0,02	30 30	BR* ESR*	30 30	14 56	70
	*siehe Seite see page 16	13							



BBC/KRUPP	THTR-BESCHICKUNGSANLAGE THTR-FUELLING PLANT	ABB. 1 FIG. 1


VERZÖGERUNG
REAKTOR
ABZUG
SCHROTTBEHÄLTER
ZUGABE
SICHTMASCHEN
SCHLEUSE
STAUBFILTER
FÖRDERGEBLÄSE
SCHLEUSENVENTIL
VEREINZELER
SCHROTTABSCHEIDER
ZÄHLSPULE
HALTEKLINKE
DOSIERER
SAMMLER
SCHNELLSCHLUSSVENTIL
REPARATURARMATUR
DOSIERER / DRUCKSPERRE
HÖHENFÖRDERER
WEICHE
TRIMMARMATUR
DURCHFLUSSMESSUNG
ABBRANDMESSUNG
UNTERSCHEIDUNGSMESSUNG
SCHLEUSE
FÖRDERUNG
BBC / KRUPP
BRENNELEMENTKREISLAUF
FÜR 300MW - KERNKRAFTWERK
THTR



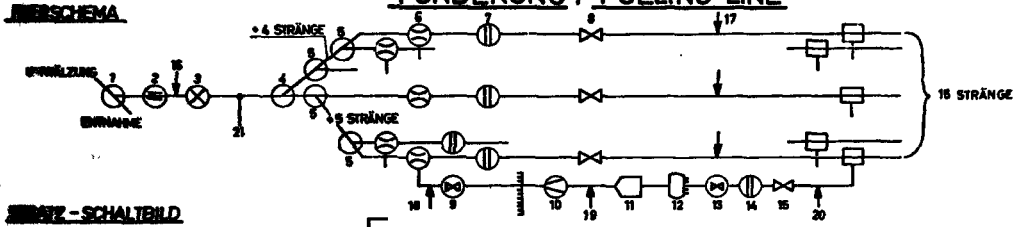
C / KRUPP

FUNKTIONSTEILEANORDNUNG
REFUELING MECHANISMS ASSEMBLY

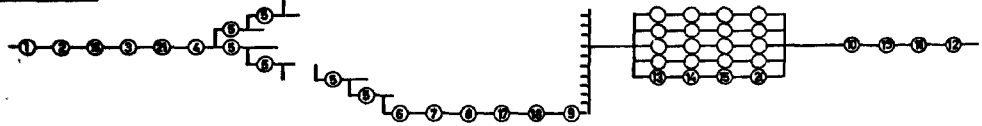
THTR
ABB. 3

FÖRDERUNG / FUELING LINE

FLIESSCHEMA

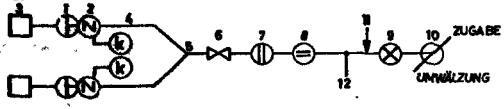


ERSATZ - SCHALTBILD

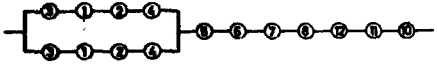


ABZUG / EXTRACTION LINE

FLIESSCHEMA

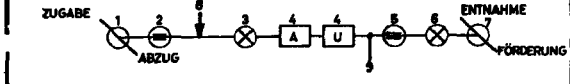


ERSATZ - SCHALTBILD

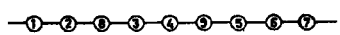


UMWÄLZUNG / CIRCULATION LINE

FLIESSCHEMA



ERSATZ - SCHALTBILD

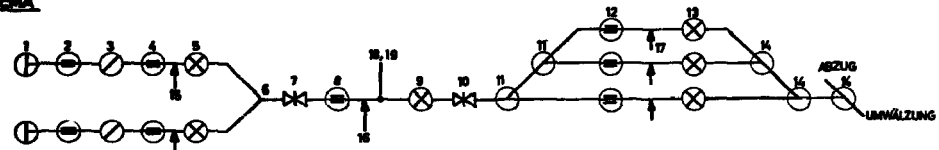


SCHROTTKANNE

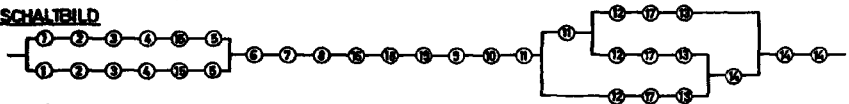
Gez. 18.8.69 Stefan Gepr.: BBC/KRUPP	BESCHICKUNGSANLAGE THTR FUELING PLANT THTR	Abt.-Zeich.: ZCHN. NR.: GJ4 233 261 ABB. 4

ZUGABE / SUPPLY - LINE

FLIESSCHEMA

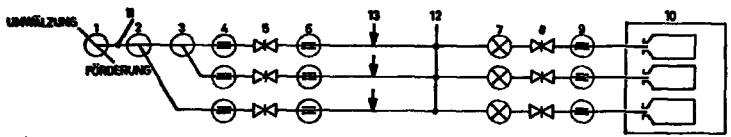


ERSATZ - SCHALTBILD

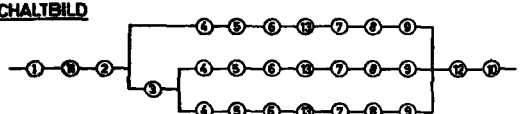


ENTNAHME / DISCHARGE - LINE

FLIESSCHEMA



ERSATZ - SCHALTBILD



Gez.: 18.8.69	BESCHICKUNGSANLAGE THTR	Akt.-Zeich.:
Gepr.:	FUELING PLANT THTR	ZCHN. NR.: GJ4 233 260
BBC/KRUPP		ABB. 5

246

DEMONSTRATION OF THE PERFORMANCE AND RELIABILITY OF THE GENERAL ELECTRIC CO. BOILING WATER REACTOR MAIN STEAMLINE ISOLATION VALVES

by

I. M. Jacobs

Atomic Power Equipment Dept.
General Electric Co.
San Jose, California, U.S.A.

Prepared for presentation at the CREST meeting.
Reliability of Mechanical Systems and Components
Risø, 24th - 26th, September, 1969

DEMONSTRATION OF THE PERFORMANCE AND RELIABILITY OF THE GENERAL ELECTRIC CO. BOILING WATER REACTOR MAIN STEAMLINE ISOLATION VALVES

by I. M. Jacobs

INTRODUCTION

The General Electric Company has used reliability analysis and assessment techniques to evaluate critical designs since the beginning of its commercial power venture. The emphasis has been on performing trade-off studies during the early stages of design to select a system configuration with adequate reliability potential, first on instrumentation and logic[1 2 3]; later expanded to include complete systems for emergency cooling[4]. Other valuable studies have assesed the effect of test frequency and repair time[5 6] on the availability and reliability of engineered safeguards.

In any reliability analysis, there is always concern that the meager failure rate data available actually represents the failure rate of a particular component in a particular environment. A case in point is the main steam isolation valve which was originally designed for closing against a flow of saturated or superheated steam. This type of valve has a good performance record and wide acceptance in industry. The question to be resolved is this: Does the valve perform equally well for the expected conditions following a postulated break of a main steam line?

A few facts will place the problem in perspective. In the General Electric direct cycle Boiling Water Reactor (GEBWR), the steam lines couple the reactor directly to the turbine. In the event of a postulated steam line break outside the primary containment, an escape path is present for loss of reactor steam and water and any dissolved radioactive materials carried with them. For sufficiently large breaks, this loss of reactor coolant, if unchecked, would result in the release of a large fraction of the vessel fluid. Two isolation valves are provided in each main steam line for the express purpose of providing a redundant means for terminating such a coolant loss without uncovering the reactor core.

To meet the safety needs as well as the requirements for low pressure drop during normal plant operation, a Y-type design was selected which uses an air cylinder operator and closing spring as separate independent closure devices. Individual design features of this design include a basic stop-check configuration, pilot valves, closing springs, air operator, and oil dash pot. All of these individual features have wide acceptance in industry. The total combination of these features, however, had not been tested under the combination of conditions postulated for the steam line break accident. This combination of conditions may include very high steam flow rates, high velocity steam-water mixtures, and dynamic loadings in addition to the static pressure differentials. Proper and rapid closure of the isolation valves under these conditions is a safety function in the plant, and

---

* I. M. Jacobs is a Reliability Engineer in the Atomic Power Equipment Dept. of the General Electric Co., San Jose, California.

the concern was simply that valves of this type and large size had not demonstrated their performance and reliability under accident conditions. However, analysis of the conditions and examination of the valve design, together with a number of specification tests possible under shop conditions, provided significant assurrance that the valve performance would be satisfactory. Never-the-less, a large-scale demonstration was considered desirable to establish greater confidence in the ability of the valve to perform reliably.

THE DEMONSTRATION PROGRAM

The approach taken was to test a typical full-size valve under conditions which approximate as closely as possible the most severe conditions the valve is predicted to experience in the event of a steam line break outside the drywell. The primary objective was to demonstrate proper closure of the valve under such conditions. In addition, some tests were made at conditions more severe than expected to demonstrate ample safety margin.

A two-phase flow analysis of the postulated accident was performed to provide the expected conditions of pressure, flow rate, and quality at the valve. This information was utilized to plan the experiment and to design the test facility to provide the wide range of conditions needed. The test facility was built in the Commonwealth Edison Company's State Line Station Unit 1 and utilized the full steaming capacity of all boilers with a total thermal rating of approximately 700,000 KW at a nominal pressure of 650 psig. A specially fabricated set of headers and valves allowed for mixing steam and water from one or more of the six boilers prior to admission to the valve under test. The steam headers ranged in size from 14 inches to 20 inches with venturi sections built in to measure steam flows.

The main steam isolation valve tested was an air-and-spring operated Y-pattern globe valve for use in a 20 inch pipeline (Figure 1). The valve tested was taken off the production line and is typical of the valves used in GE-BWR's.

Each test was initiated by quickly venting a balancing pressure from between a pair of rupture discs which simulated the instantaneous rupture of the steam line. The test valve was closed on a variety of flow conditions covering the following ranges:

Steam only tests:	50 to 1080 lb/sec	
Water only tests:	240 to 3490 lb/sec	
Mixture tests:	1530 to 3860 lb/sec	(quality range 0.17 to 0.45)
Surge tests:	520 to 2970 lb/sec	(quality range 0.01 to 0.33)

RESULTS

The main steam isolation valve under test was opened and closed without fail more than 400 times (200 cycles) during the two-month test program. It shut off more than 40 flow tests which simulated accident conditions including those more severe than postulated for the design basis accident in the nuclear power plant. Each time it opened and closed when signaled and shut off the flow completely and reliably.

Figure 2 shows the differential pressure when a saturated steam/water mixture flows through the valve part way through its closing stroke, as may occur in the event of a steam line break. A gradual rise in differential pressure is observed as the valve closes on steam flow. When mixture enters the steam line a decrease in pressure occurs at the valve followed by a slight overshoot at the time of transition from steam flow to mixture flow at the valve. Eighteen of these surge pressure runs were included in the test program. Contrary to original concerns and conservative predictions that very large pressures might accompany the surge of fluid (rapid transition from steam to steam-water mixture) through the valve, the tests demonstrated that the surge pressures were minor and entirely within the rated boiler pressure.

The test demonstrated that steam and mixture flows assisted valve closure. Closing speeds during the flow tests were generally 20% faster than the closing speed under cold, atmospheric pressure conditions.

Analysis of closing performance on this wide variety of conditions demonstrated that valve closure is not critically sensitive to temperature, pressure, fluid in the valve, or fluid flow.[7]

CONCLUSIONS

The pressure and flow transient response in the steam line during the postulated external steam line break accident condition can be analytically predicted and the type of commercially available main steam isolation valves used in boiling water reactor nuclear power plants designed by the General Electric Company will close as required under the steam and two-phase mixture flow conditions that could occur for the design basis accident. To the reliability analyst, it is significant that this standard valve did not fail during more than 200 cycles of operation, over 40 of them in simulated accident conditions. Even more significant, this valve was drawn from a larger population of valves which over the years have demonstrated reliable performance in normal steam service conditions. These tests have demonstrated that the valve is not overstressed and is capable of operation with mixed steam and saturated water flow conditions. Thus it seems reasonable to use generic failure rate data in a reliability analysis of the main steam line isolation valve function.

ACKNOWLEDGEMENTS

This report is based on work performed by others. Personnel in Design Engineering planned the program and designed the test facility. Personnel in Development Engineering conducted the tests and analyzed the results. The Commonwealth Edison Co. provided the use of their State Line plant as a steam source and test facility.

REFERENCES

[1]Safety Systems for Nuclear Power Reactors, I. M. Jacobs, Communication and Electronics, American Institute of Electrical Engineers, Number 33, November, 1957, pp. 670-673.

[2]Safety System Design Technology, I. M. Jacobs, Nuclear Safety, Volume 6, No. 3, Spring 1965, pp. 231-245.

[3]Reactor Protection System -- A Reliability Analysis, I. M. Jacobs, APEC-5179, June 1966, General Electric Company.

[4]Emergency Core Cooling System Availability Analysis, Dresden Nuclear Power Station Units 2 and 3 Safety Analysis Report, Section 6.2.7.4.

[5]Reliability of Engineered Safety Features as a Function of Testing Frequency, I. M. Jacobs, Nuclear Safety, Vol. 9, No. 4, July-August 1968.

[6]Guidelines of Determining Safe Test Intervals and Repair Times for Engineered Safeguards, I. M. Jacobs and P. W. Marriott, APEC-5736, April 1969, General Electric Company.

[7]Design and Performance of General Electric Boiling Water Reactor Main Steam Line Isolation Valves, APED-5750, D. A. Rockwell and E. H. vanZylstra, March 1969, General Electric Co.

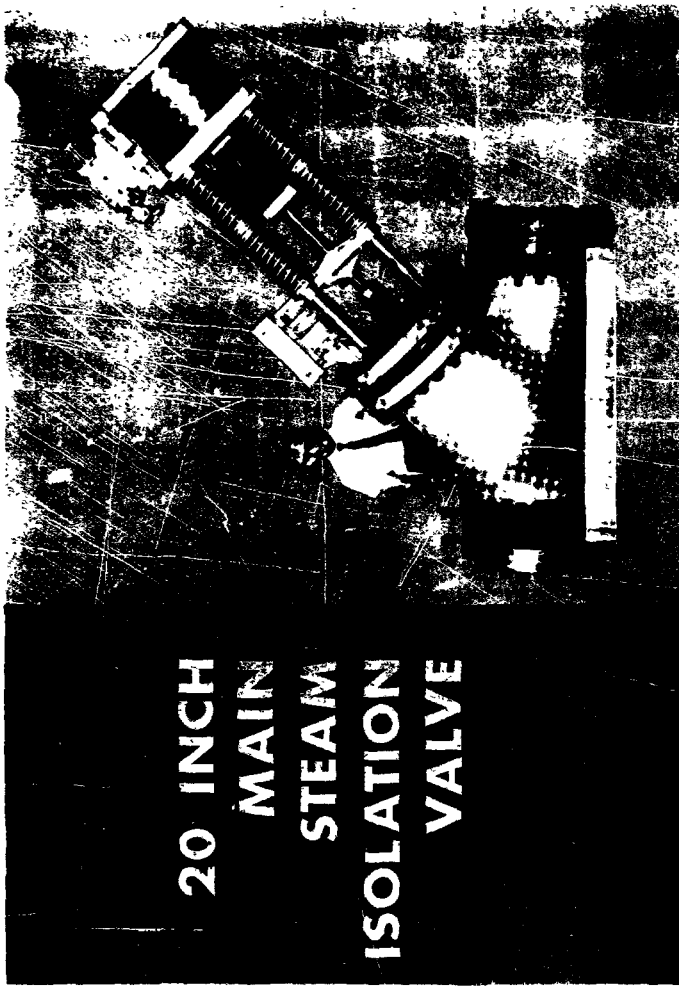


FIGURE 1

PRESSURE DIFFERENTIAL RESPONSE AT VALVE

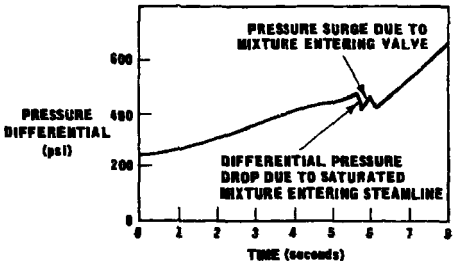


FIGURE 2

THE COMMISSION OF THE EUROPEAN COMMUNITIES
E U R A T O M
JOINT NUCLEAR RESEARCH CENTER
ISPRA ESTABLISHMENT (ITALY)

FRACTURE MECHANICS APPROACH TO THE ASSESSMENT OF RELIABILITY OF REACTOR PRESSURE TUBES

by

D. BASILE(*), G. VOLTA

Meeting of Specialists on the Reliability of
Mechanical Components and Systems for
Nuclear Reactor Safety

RISØ, 24th-26th September 1969

(*) now at AGIP-Nucleare.

1. Introduction

One of the main factors which affect the lifetime of Zirconium components in nuclear reactors is the embrittlement by radiation and hydrogen pick-up.
The quantitative evaluation of this factor and its implications in the assessment of safety are still matters of discussion.

The development of the science of fracture mechanics has produced methods and criteria for a quantitative evaluation of the brittleness of the basic material.
But great difficulties arise when we want to estimate the mechanical stability of the whole structure, given certain properties of the basic material.
In fact the risk of a catastrophic failure due to the brittleness supposes the presence of flaws or cracks. The distribution of the cracks and the dimensions of the largest one, depends on the dimensions and the complexity of the item considered, on the age, on the controls, etc.. This means that the risk of a catastrophic failure is connected to several factors which are of a statistical nature.

Usually the factor "embrittlement" is considered alone and overemphasized, while inadequate attention is given to the interconnection of all the factors. The reason is that other factors can be estimated only with reference to single engineering components and a statistical treatment is needed.

This paper gives an example of how different factors can be statistically considered together in order to estimate the catastrophic failure probability of a structure like a pressure tube in Zirconium alloy.
Also given are the heuristic possibilities of the method when simplified assumptions about factors and their variability are made.

2. Basic concepts and formulas

Given a component and the type of failure let $F_R(x)$ be the

probability that the resistance to failure of the component is less than a certain x and $F_C(x)$ the probability that the load which causes the failure is greater than x, these probability distributions being a function of time.
The failure will occur when $x_C > x_R$.
Therefore the probability of failure or unreliability is expressed by (Fig. 1) :

$$(1) \qquad H(t) = \int_0^\infty \left| F_R(x,t) \frac{\delta F_C(x,t)}{\delta x} \right| dx$$

The reliability will be :

$$(2) \qquad R(t) = 1 - H(t)$$

It is useful to introduce another xoncept is some way analogous to "safety factor" in the conventional calculation methods.
The "safety factor" is the ratio of the resistance to the load.
We introduce a "load factor" :

$$(3) \qquad y = \frac{x_R}{x_C}$$

where x_R and x_C are quantities statistically distributed. Therefore y will also be statistically distributed.
Given $F_R(x)$ and $F_C(x)$, the distribution of y is expressed by :

$$(4) \qquad F(y) = P\left(\frac{x_R}{x_C} < y\right) = \int_0^\infty \left| F_R(yx_c \left(\frac{\delta F_C(x_c)}{\delta x_c} \right| d x_c$$

For y = 1 the value of F(y) corresponds to the probability of failure, i.e. the probability of failure corresponds to the probability of a load factor = 1.

Formulas (1) and (4) summarize the whole of structural reliability theory.

The use of these formulas supposes the knowledge of the distribution function $F_R(x)$ and $F_C(x)$.

Moreover, the solution of (1) and (4) in a finite form is not possible except for very few distribution functions.
For this reason the literature usually gives a simplified approach [1, 2] based on the error propagation theory.
According to this approach instead of the distribution function, only the variances are considered.
Let Z(m,n) be a function of the statistically distributed variables m and n.
A Taylor's series expression of Z can be written :

$$(5) \qquad Z(m,n) = Z(m_o, n_o) + \frac{\delta Z}{\delta m}\Big|_o (m - m_o) + \frac{\delta Z}{\delta n}\Big|_o (n - n_o) + \ldots$$

If the higher order terms are neglected :

$$(6) \qquad Z(m,n) \; a + b\, m + c\, n$$

Regard less of the type of distribution of m and n, the variance will be given by :

$$(7) \qquad var^2 (Z) = b^2\, var^2 (m) + c^2\, var^2 (n)$$

This formula implies that a change in Z can be estimated as a linear function of the changes in the individual variables.
For instance, given the variances of load and resistance the variance of the load factor can be easily estimated.
However to have numerical values of probability we need the distribution law. When m and n follow a normal distribution, Z also follows a normal distribution. But when m and n follow another type of distribution, the correct distribution for Z can only be obtained by formulas like (4). Hence, the simplified approach can give in this case only a qualitative indication.

3. Outline of the model adopted for the reliability calculation

Starting from the basic concepts referred to previously, the following reliability midel for our structure is assumed.
The failure considered is the catastrophic failure due to the brittle propagation of a crack.
For our tube a certain distribution of defect size is assumed. The relationship between the critical defect size and the corresponding applied stress allows the derivation of the resistance distribution. Then the load or applied stress distribution is assumed. By the superposition of the applied load distribution to tee resistance distribution in (1) the reliability is calculated.
The distributions F_R and F_C are considered variable with time, i.e. their parameters are function of time.
The effect of the inspections aiming at limiting the maximum crack size and the maximum load value can be expressed by a variation of the extremes of the integral (1) i.e. by a truncation of the distributions F_R and F_C.

4. Main characteristics of the actual structure.

The specific considerations that follow refer to pressure tubes of Zr 2,5 % Nb alloy to be installed in the experimental zone of the Essor reactor (fig. 2).
Tensile properties of the materlal are given in tab. 1.
From the coolant which is planned to be used in the loops (water or organic coolant) we expect significatant hydrogen pick-up at the operating conditions (up to 300°C for water and 360°C for organic coolant). The embrittling effect of the hydrogen on the unirradiated material has been evaluated by C.O.D. test on a SEN specimen (fig. 3).
To clarify the meaning and the reason for this test we recall the general relationship between the critical length "a" of a crack line defect and the applied stress :

$$(8) \qquad \sigma \cdot a^n = B$$

where B is a constant which characterizes the material from the point of view of the brittleness and n is an exponent which can vary from 1/2 to 1.
In the case of a plane sheet loaded in a direction perpendicular to the defect length, B is proportional to the "Fracture Toughness" or "Crack Extension Force" G_c, i.e. to the energy needed to propagate the fracture of a surface unit.
In the case of tubes loaded by internal pressure and containing axial defects, B is still a quantity characteristic for the material, but is not related only to the "Fracture Toughness" because we are far away from the conditions of validity of "linear elastic fracture mechanics".
In general the relationship (8) can be experimentally determined by a burst test on artificially flawed tubes. As this type of test is very expensive, a great effort has been made to attempt to discover small tests from which a reliable extrapolation to tubes would be possible.
A technique, based on the assessment of the crack opening displacement δ in the region near the tip of a defect, gives within certain limits satisfactory results [3].
The relationship between C.O.D., the hoop stress in the tube and the length of the corresponding critical defect is given by :

$$(9) \qquad \delta = \frac{\pi}{E} \frac{\sigma^2}{\sigma_y} a$$

where

σ_y = yielding stress

E = Young's modulus

The formula (9) corresponds to (8) with n = 1/2.
C.O.D., δ , can be measured on small specimens.
From the values of C.O.D., for each material condition, the constant B is derived :

$$(10) \qquad B = \left(\frac{\delta E \sigma^2}{\pi} \right)^{1/2}$$

The values of δ , measured on our material, versus the hydrogen concentration, at room temperature, is given in fig. 4.
The values of δ depend on the crack orientation due to the texture of the tube material.
We have considered the C.O.D. corresponding to the longitudinal defect, the most dangerous and the most probable in our situation.
The values of C.O.D. increase very rapidly with the temperature, so that the most dangerous condition for our material is low temperature.
This is why we assume room temperature for our calculations.
An embrittlement effect should be expected also from the neutron irradiation. The fast flux (> 1 Mev) on our tube is of the order of $5 \div 10.10^{13}$ n/cm^2 sec.
In one year we have already a dose of the order of 10^{21} n/cm^2.
Like the hydrogen, irradiation has no detrimontal effect on the tensile and yield strength, of Zirconium alloys, while significant effect has been observed on impact properties and fracture toughness.
However this effect tends to a saturation at a dose of 10^{21} n/cm^2.
It could be equivalent to a hydrogen concentration of 100 - 150 ppm.
The superposition of the radiation effect on the hydriding effect is not additive.
The impact properties and the fracture toughness tends to have a limiting absolute value [4].
Specific tests are underway at HFR (Petten).
In the absence of definitive experimental data various hypotheses have been made (fig. 5). The curve (3) is considered the most probable. It corresponds to a rate of embrittlement equivalent to an hydrogen pick-up of 300 - 400 ppm after 20 years. The linear variation with time has been assumed for simplicity as a first approximation.

5. Determination of F_R (x,t)

5.1. Flaw distribution

Let F(a) be the probability that the largest longitudinal defect in the tube is longer than "a".

We choose for F(a) a Weibull distribution.
At present experimental data on defect size and on their statistical distribution are very poor, and the choice of a Weibull distribution is arbitrary. However it can be justified on the one hand by the formal advantages of this two parameter distribution and on the other by the fact that this type of distribution has been successfully adopted in similar cases :

$$(11) \qquad F(a) = e^{-(\frac{a}{a_o})^{\beta}}$$

β and a_o are respectively the form and the scale parameters of the distribution.

5.2. Resistance distribution

According to (8) we can write (11) replacing "a" by :

$$(12) \qquad F(\sigma) = e^{-(\frac{\sigma}{\sigma_o})^{-\beta/n}}$$

$F(\sigma)$ expresses the probability that the resistance is lower than σ, i.e. the probability that the largest defect present is lohger than the defect a for which σ is critical.
The constant B of the material is included in the parameter T .
Consider now that the basic material is embrittled keeping constant the cracj distribution i.e. the parameter σ_o.
The basic material will be characterized by a new $B' < B$.
If we indicate $\alpha = \frac{B'}{B}$ the new parameter σ'_o to be introduced in (12) according to (8) will be :

$$(13) \qquad \sigma'_o = \sigma_o \cdot \frac{B'}{B} = \sigma_o \, \alpha^n$$

The new resistance distribution is :

$$(14) \qquad F'_R(\sigma) = e^{-(\frac{\sigma}{\sigma_o \alpha^{-n}})^{-\beta n}} = \left[F_R(\sigma) \right]^{\alpha\beta}$$

If we plot on loglog paper ln $F_R(\sigma)$ versus $\frac{\sigma}{\sigma_o}$ we have a straight line :

$$(15) \qquad \text{logln } F_R(\sigma) = -\frac{\beta}{n} \log \frac{\sigma}{\sigma_o}$$

A variation of the properties of the material keeping constant the crack distribution corresponds to a vertical translation of a quantity log :

$$(16) \qquad \text{logln } \frac{1}{F_R'(\sigma)} = \text{logln } \frac{1}{F_R(\sigma)} - \beta \log \alpha$$

To introduce the variable time we write (12) and (14) in the form :

$$(17) \qquad F_R(x,t) = e^{-K_{r_1} x^{-m_r(t)}}$$

$$(18) \qquad F_R'(x,t) = e^{-K_{r_1} \alpha(t)^{n.m_r(t)} x - m_r(t)}$$

As we have supposed that the parameter (t) expressing the embrittlement of the basic material is linear with time (fig. 5), we can write :

$$(19) \qquad K_r(t) = K_{r1}(1 - (t-1)\, C_1)^{n\, m_r(t)}$$

where

$$(20) \qquad C_1 = \frac{1 - \alpha(t)}{t - 1}$$

If we suppose also that the parameter $m_r(t)$ expressing the form of the distribution and therefore interpreting the phenomena connected with the modification of the crack distribution (wear, local corrosion etc..) is linear :

$$(21) \qquad m_r(t) = m_{r1} + (t-1)\, C_{dr}$$

5.3. Numerical expression of $F_R(x,t)$

We assume on the basis of fabrication experience some points are fixed and on them the Weibull distribution is drawn :

(22) $F(a) = e^{-990\ a^{1,075}}$

From this distribution we derive the parameters K_{r1} and m_{r1}

(23) $K_{r1} = 990$

(24) $m_{r1} = 2,15$

As a variable w we take

(25) $x = \frac{\sigma}{\sigma_N}$

where σ is the actual hoop stress and σ_N the nominal allowable stress calculated in accordance with the ASME code for pressure vessel :

(26) $\sigma_N = \frac{\sigma_R}{3}(300°C) = 16\ kg/mm^2$

From the fig. 4 which gives the C.O.D. at the initial time and from (9) the resistance distribution at the initialtime time is derived :

(27) $F_R(x) = e^{-990\ x^{-2,15}}$

In fig. 6 are plotted such distributions.

To fix (21) the following hypotheses are made about the evolution of the probability distribution.
We suppose that in time the probability of the almost incredible defect remains constant and the probability of shorter cracks increases (fig. 7).

As several phenomena can contribute to the growing of the defects (wear, pressure cycling, thermal fatigue) various values are also assumed for the parameter C_{dr}.
We have plotted in fig. 6 the crack distributions after 20 years of operation for various C_{dr}.
To give the physical meaning of these values we can see that they correspond to a probability for a crack larger than 6 mm after 20 years of 10^{-7}, 10^{-4} and 10^{-1} respectively.

6. Determination of $F_C(x,t)$

As we have already said $F_C(x,t)$ is the probability that the maximum applied stress attained in the time t is higher than x. The variable x os still $\frac{\sigma}{\sigma_N}$ (25).

We assume also for this distribution a Weibull type :

$$(28) \qquad F_C(x,t) = e^{-K_c(t)\ x^{\ m_c(t)}}$$

This distribution will change in time in the sense that the probability of having m load higher than a certain x is increasing with the time.
We assume that the time affects mainly the probability of having accidental overload, i.e. the distribution on the side where the probability values are very low, so that no change can be considered of the distribution around the value x = 1.
With this hypothesis we can write $K_c(t) = K_c(1) = \text{constant}$.
To take into account the timewise increasing probability of values of x higher than 1, $m_c(t)$ is expressed as a linear function of the time :

$$(29) \qquad m_c(t) = m_{c1} - (t-1)\, C_{dc}$$

Numerical values for the constants K_c and m_{cl} can be obtained on the basis of an analysis of all the possible plant operation conditions. C_{dc} is a parameter which expresses the reliability of the safety devices foreseen to keep the loading conditions below certain levels.
In fig. 6 F_C is plotted for the following values of the parameters :

$K_c = 2,"$
$m_{cl} = 4,4$
$C_{dc} = 0,135$ and $0,07$

This corresponds to the following probabilities

$t = 1$ year
$P\ (x=1) = 10^{-1}$
$P\ (x=1,5) = 3.10^{-7}$
$P\ (x=2) = 10^{-25}$
$t = 20$ years
$P\ (x=1) = 10^{-1}$
$P\ (x=2) = 10^{-8}$ and 6.10^{-4}

7. Reliability calculation

The formula (1) has been solved by a digital computer programme for the distributions indicated above.
The most interesting comments on the results are in connection with the mutual effects of the four factors considered : embrittlement, flaw distribution, load distribution, control limiting the maximum defect size.

In fig. 8 to 13 are given different cases considered.

In table 2 are given the values of the reliability for different values of the parameter expressing embrittlement, flaw distribution, load distribution and truncation.

The following remarks can be made on the results :

a) The embrittlement can modify the reliability of a structure more or less according to the kind of crack and load distribution we can expect in the structure.

The degradation phenomena are not additive in a simple way.

A structure with a high standard regarding the probability of cracks has a reliability much more sensitive to a basic material degradation than a structure for which a great dispersion of the possible defects is supposed.

The same remark applies to the load distribution : a stringent specification on overload probabilities, which means a high reliability of the safety devices, emphasizes the effect of embrittlement.

b) When we fix certain values of reliability for pressure tubes (see for example [5] we must pay attention to the fact that, for given operating condition and inspection rigour, a very small variation of the fracture properties of the basic material can result in a variation of an important factor in the reliability. For instance in tab. 2 we sae that a variation of a factor 2 in C.O.D. which corresponds to a variation of fracture toughness of 1,4, can change the reliability from 10^{-6} to 10^{-10}.

c) The slope of the probability of failure or unreliability as a function of time tends to change.
This also can be considered a combined effect of the "evolution" of the statistical distributions determining the reliability value.

d) The positive effect of inspections in limiting the value of the maximum crack is important for the smaller times but decrease rapidly as the time increases. If what we want is a certain mission reliability for the time t, the type and the rigour of the inspections must be optimized with regard

to the particular situation and time to avoid performing ineffectual inspections and thereby wasting money.

8. Comparison with conventional methods of resistance evaluation

The conventional methods of calculation based on pressure vessel codes cannot take into account the factor "embrittlement" if no corresponding variation of tensile properties exists.
The factor "statistical distribution" of defects and of applied stress are considered in the "safety coefficients".
More recently calculation methods in which the brittle fracture alone is considered have been introduced [6]. They are based on fracture mechanics and go under the name of "leak before break criterion".
From experience in fracture testing of thin wall pressure vessels, it was reasoned that a through-the-thickness crack, normal to the maximum membrane stress, of a total length equal to twice the wall thickness would deform sufficiently under pressure to permit leakage of the pressurization medium, provided that this length was less than the critical defect size. As the leakage can be detected a critical defect of twice the thickness is considered the safe limit and the basis for the stability calculation.
According to this criterion the safety factor against brittle fracture is

$$\xi = \frac{\text{critical defect size of the operating condition}}{2 \times \text{wall thickness}}$$

In fig. 14 ξ and unreliability are plotted versus various embrittling conditions.

We can see that the quantity "safety factor against fracture" is ambiguous for values less than 2. That is to say that when the risk of brittle rupture becomes really significative only a probabilistic evaluation based on the knowledge of all factors could give a quantitative evaluation of the stability of the structure. In fact for a safety coefficient equal to one we can have an unreliability ranging from 10^{-3} to 10^{-7} according to the various cases considered.

9. Conclusions

- The reliability of a structure depends on several factors : if we take into account the statistical nature of these factors, we find that their effect on the reliability is not purely additive.
  This means that practically the same attention must be given to all the factors to avoid an error in interpreting the advantages or disadvantages in modifing one of these factors.

- The factor "embrittlement" can be estimated on the basis of fracture mechanics. But its impact on reliability has a quantitative meaning only if we refer to a determinate situation. We can say that "fracture toughness" specifications should be accompanied by a specification, on a statistical basis, of the load conditions and on the crack probability.

- The inspections must be chosen carefully, paying attention again to all the factors, including the mission time we expect from our structure.

REFERENCES

[1] "Reactor Primary Coolant System Rupture Study" Section III "Reliability Engineering"
GEAP 4964

[2] E.B. Hangon
"Statistical Methods for Structural Reliability Analysis"
Proceedings of Tenth National Symposium on Reliability and Quality Control, Washington 1964

[3] G.D. Fearnehough, B. Watkins, R.G. Mills
"Application of the Crack Opening Displacement Approach to the Prediction of Pressurized Tube Failure"
TRG Report 1348 (c)

[4] D.S. Wood, J. Winton and B. Watkins
"The Effect of Irradiation on the Impact Properties of Zirconium Alloys"
The Electrochemical Society, Fall Meeting, Buffalo, Oct. 10-14, 1965

[5] L. Cave, T.F. Williams
"Safety Assessment of Pressure Tube Heavy Water Reactors by Probability Methods"
IAEA Simposium on Heavy Water Power Reactors, September 1967

[6] R.E. Johnson
"Fracture Mechanics : a Basis for Brittle Fracture Prevention"
WAPD - TM - 505.

TABLE 1

Mechanical properties of Zirconium 2,5% Niobium heat-treated pressure tubes fabricated by Cefilac according to Euratom Specification (Unirradiated and H_2 = 20 ppm).

20°C				300°C			400°C			
σ_R kg/mm^2	$\sigma_{0,2}$ kg/mm^2	A %	S %	σ_R kg/mm^2	$\sigma_{0,2}$ kg/mm^2	A %	σ_R kg/mm^2	$\sigma_{0,2}$ kg/mm^2	A %	S %
80	58	18	56	48	38	20	44	39	22	71

N.B. With an hydrogen concentration up to 400 ppm no practical variation in σ_R, $\sigma_{0,2}$ and A is revealed. Significative variation is observed in striction.

TABLE 2

Unreliability corresponding to 20 years mission time

Case n°	Load Distribution m_c	Embrittlement / Flaw Distribution m_r	3/4	1/2	1/4	1/10	Truncation
1	1,7	2,65	$1,8.10^{-22}$	$2,2.10^{-18}$	$2,7.10^{-13}$	$3,1.10^{-9}$	
2	"	2,95	$6,2.10^{-18}$	$1,7.10^{-14}$	$2,6.10^{-10}$	$4,9.10^{-7}$	
2 a	"				$2,6.10^{-10}$		$x_{min} = 2$
2 b	"				$3,1.10^{-11}$		" = 3
2 c	"				$5,3.10^{-13}$		" = 3,5
2 d	"				$1,7.10^{-15}$		" = 4
2 e	"					$4,1.10^{-7}$	" = 2
2 f	"					$1,3.10^{-8}$	" = 3
2 g	"					$6,4.10^{-12}$	" = 3,5
2 h	"					$9,9.10^{-15}$	" = 4
3	"	3,65	6.10^{-13}	$2,6.10^{-10}$	$3,5.10^{-6}$	8.10^{-5}	
4	3	3,65	$5,4.10^{-26}$	4.10^{-19}	$1,3.10^{-10}$	$1,1.10^{-6}$	

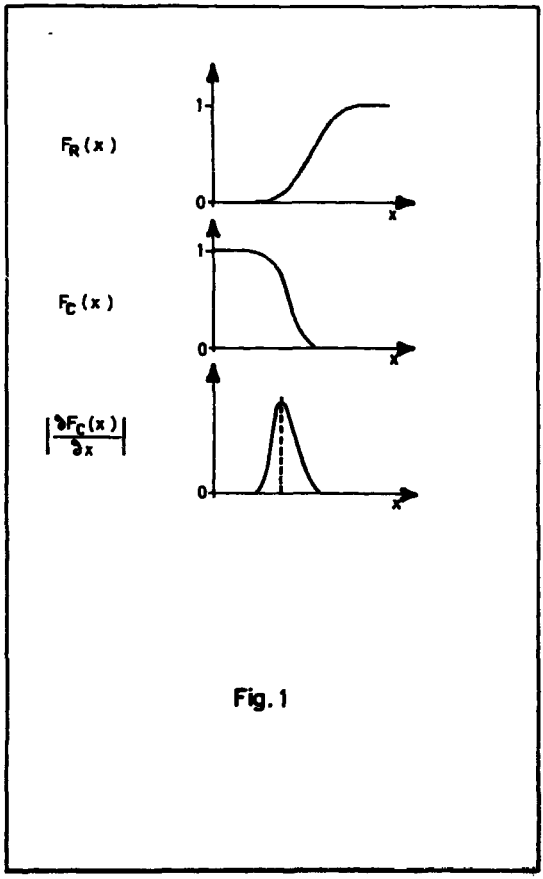


Fig. 1

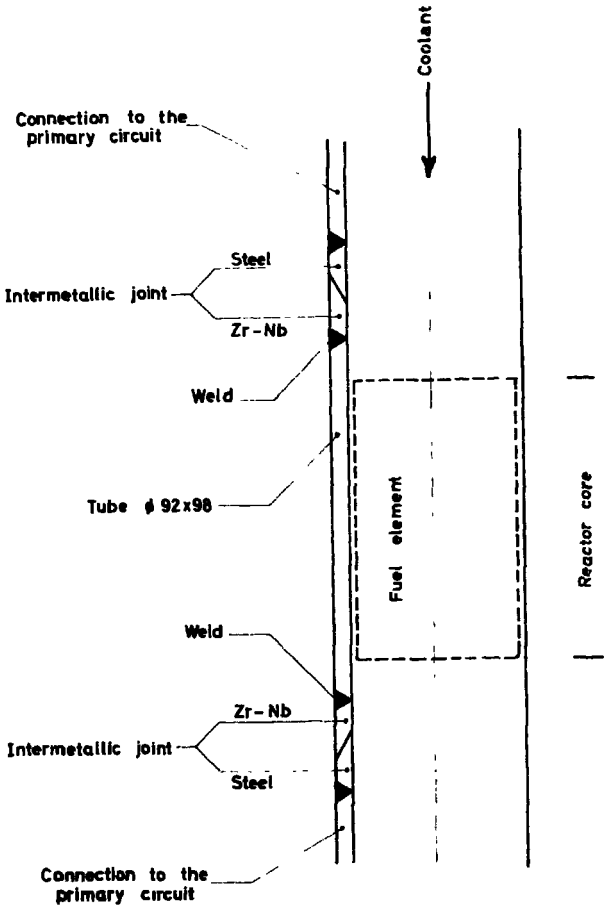

Coolant
Connection to the primary circuit
Steel
Intermetallic joint
Zr-Nb
Weld
Tube ϕ 92x98
Fuel element
Reactor core
Weld
Zr-Nb
Intermetallic joint
Steel
Connection to the primary circuit

Fig. 2

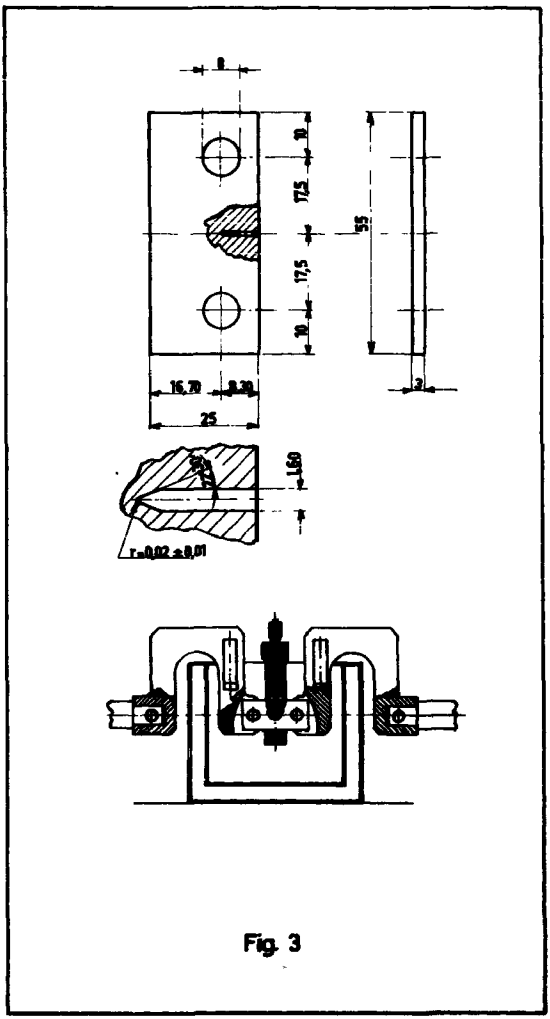


Fig. 3

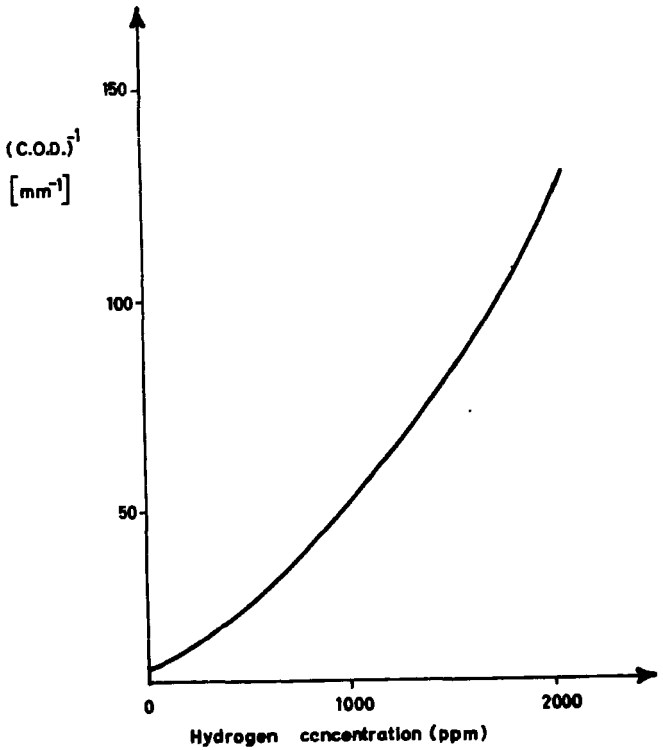


Fig.4

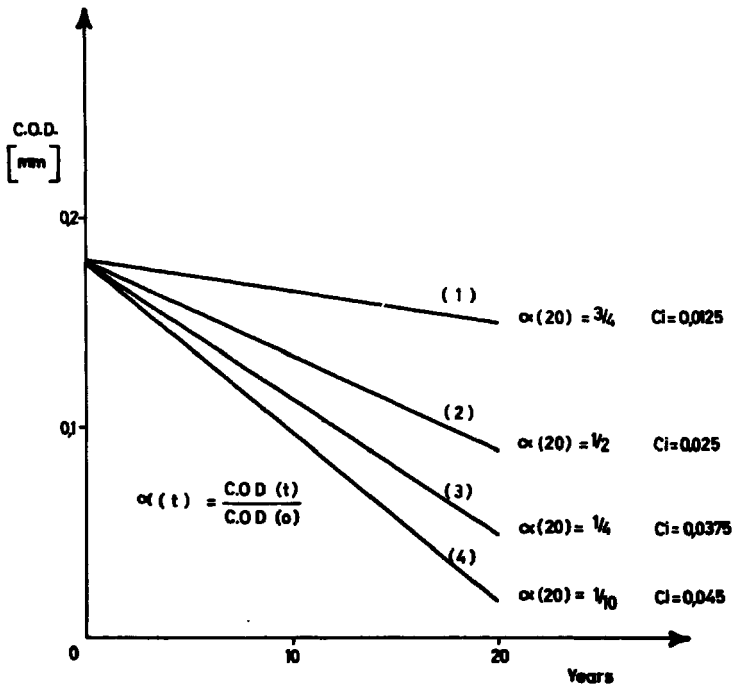

C.O.D.
[mm]
0,2
0,1
0
10
20
Years
(1)
α(20) = 3/4
Ci = 0,0125
(2)
α(20) = 1/2
Ci = 0,025
(3)
α(20) = 1/4
Ci = 0,0375
(4)
α(20) = 1/10
Ci = 0,045
α(t) = C.O.D (t) / C.O.D (o)

Fig. 5

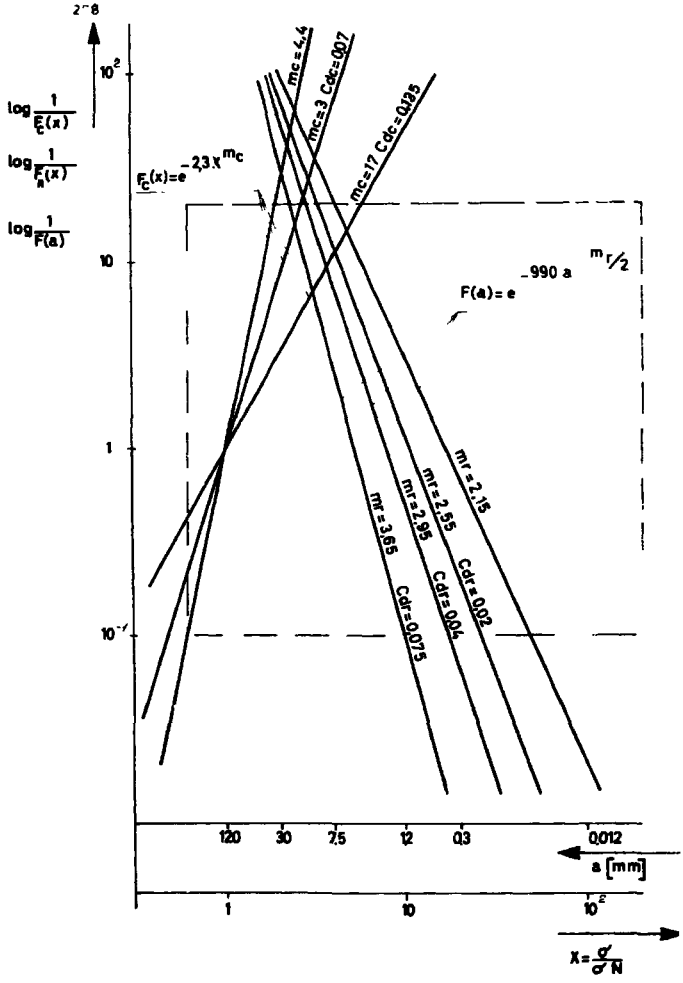
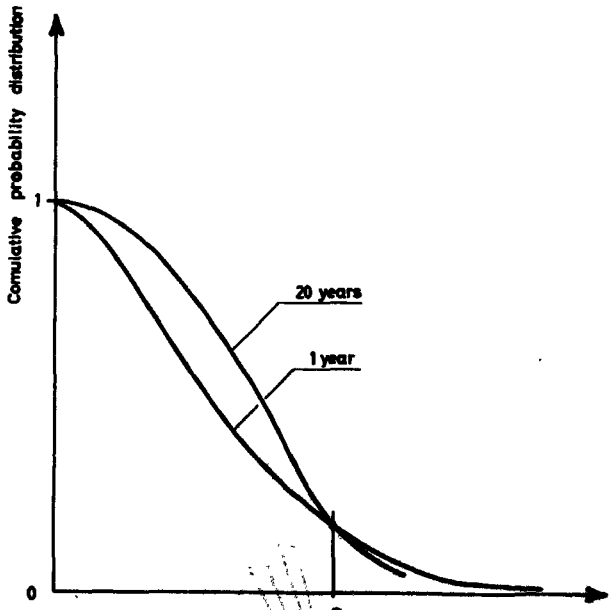

2-8
10^2
10
1
10^{-1}
$\log \frac{1}{F_c(x)}$
$\log \frac{1}{F_n(x)}$
$\log \frac{1}{F(a)}$
$F_c(x)=e^{-2,3\,x^{mc}}$
mc=4,4
mc=3 Cdc=0,07
mc=17 Cdc=0,135
$F(a)=e^{-990\,a^{mr/2}}$
mr=2,15
mr=2,55 Cdr=0,02
mr=2,95 Cdr=0,04
mr=3,65 Cdr=0,075
120
30
7,5
1,2
0,3
0,012
a [mm]
1
10
10^2
$X=\frac{\sigma}{\sigma' N}$

Fig. 6



($a^{\oplus}$ = almost incredible defect size)

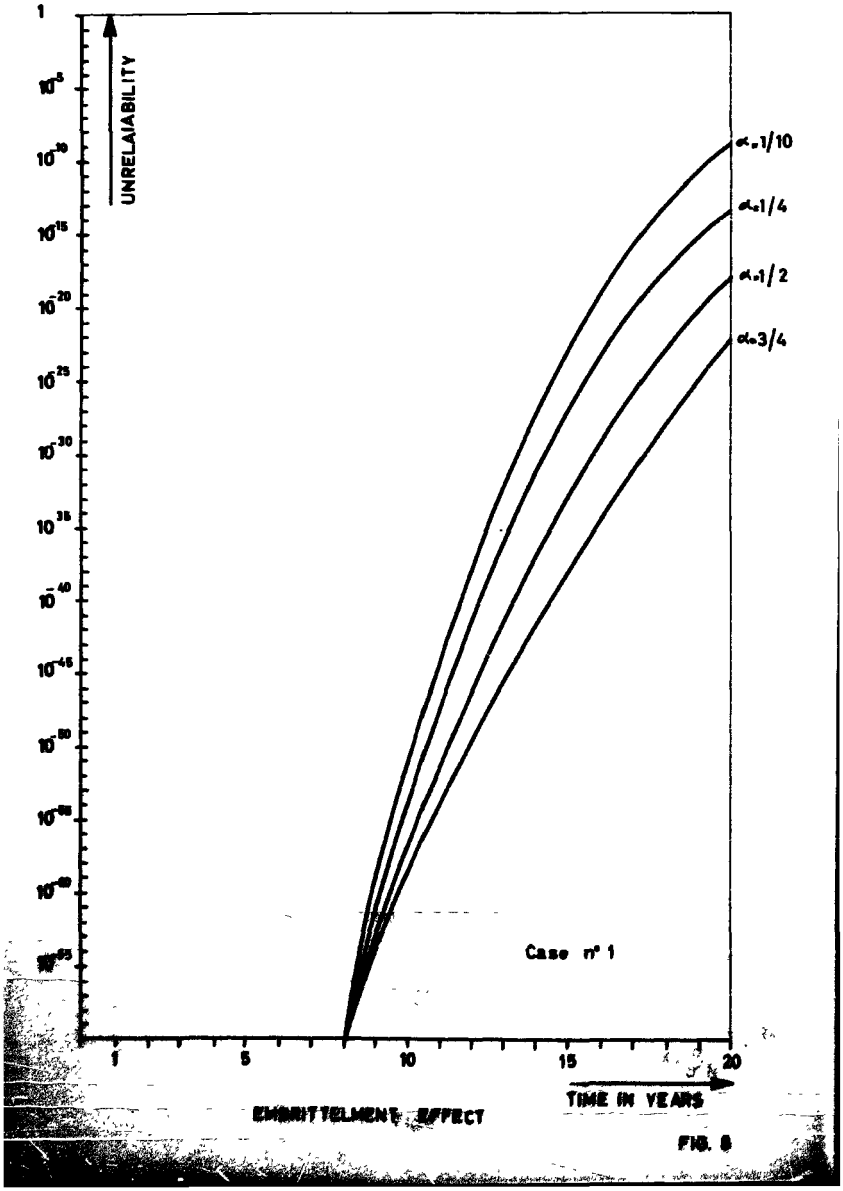
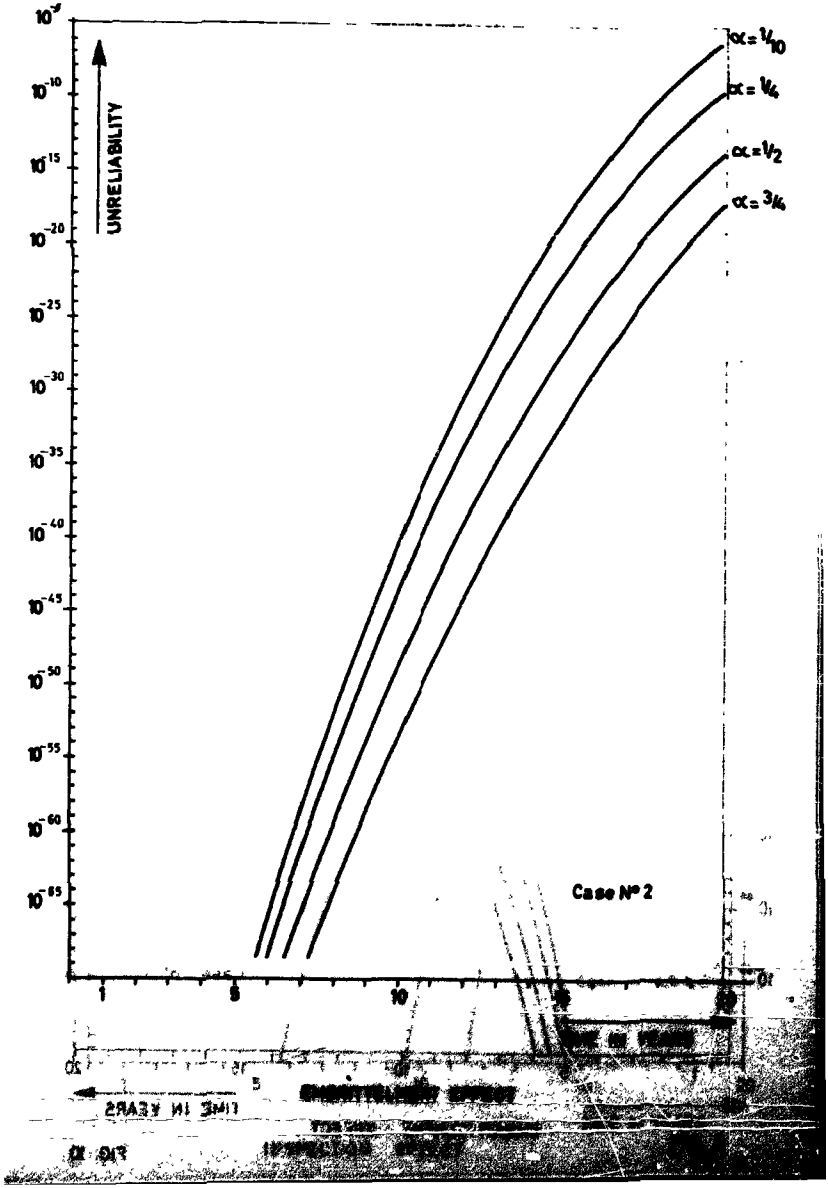
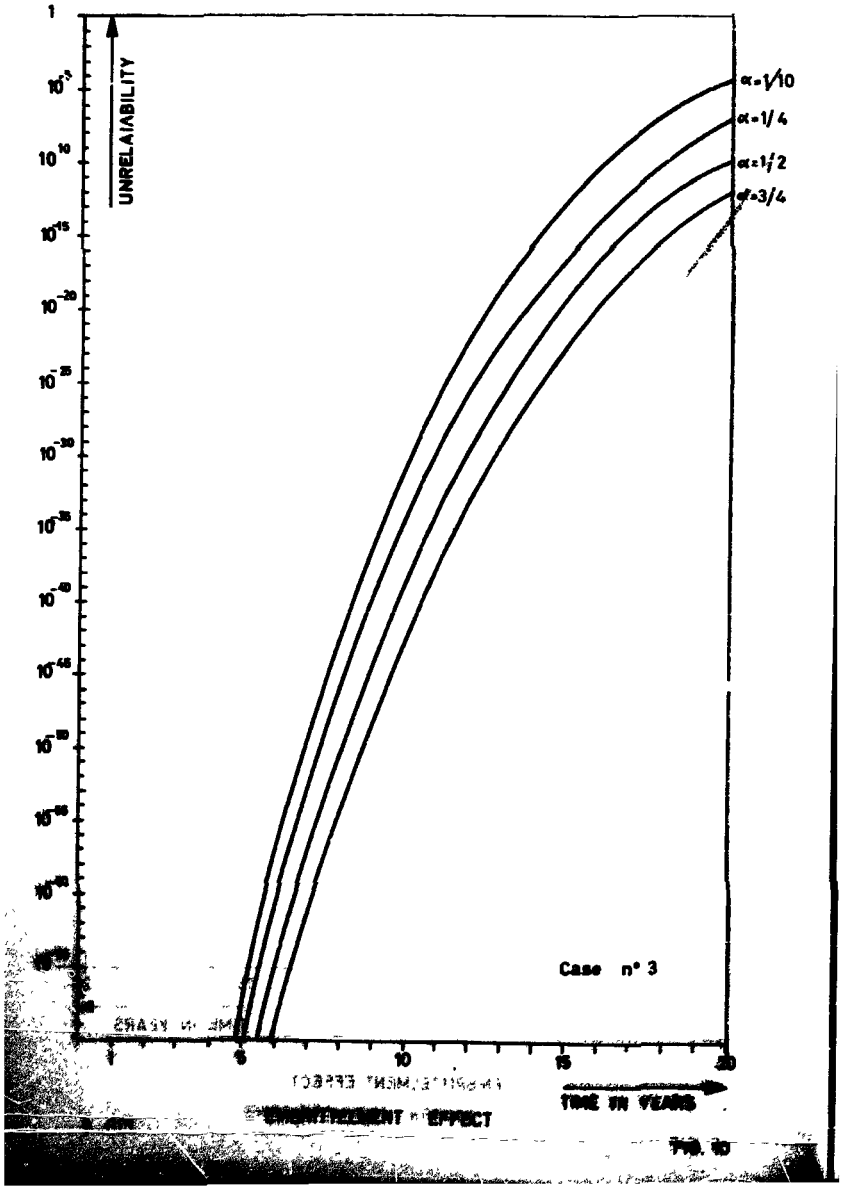
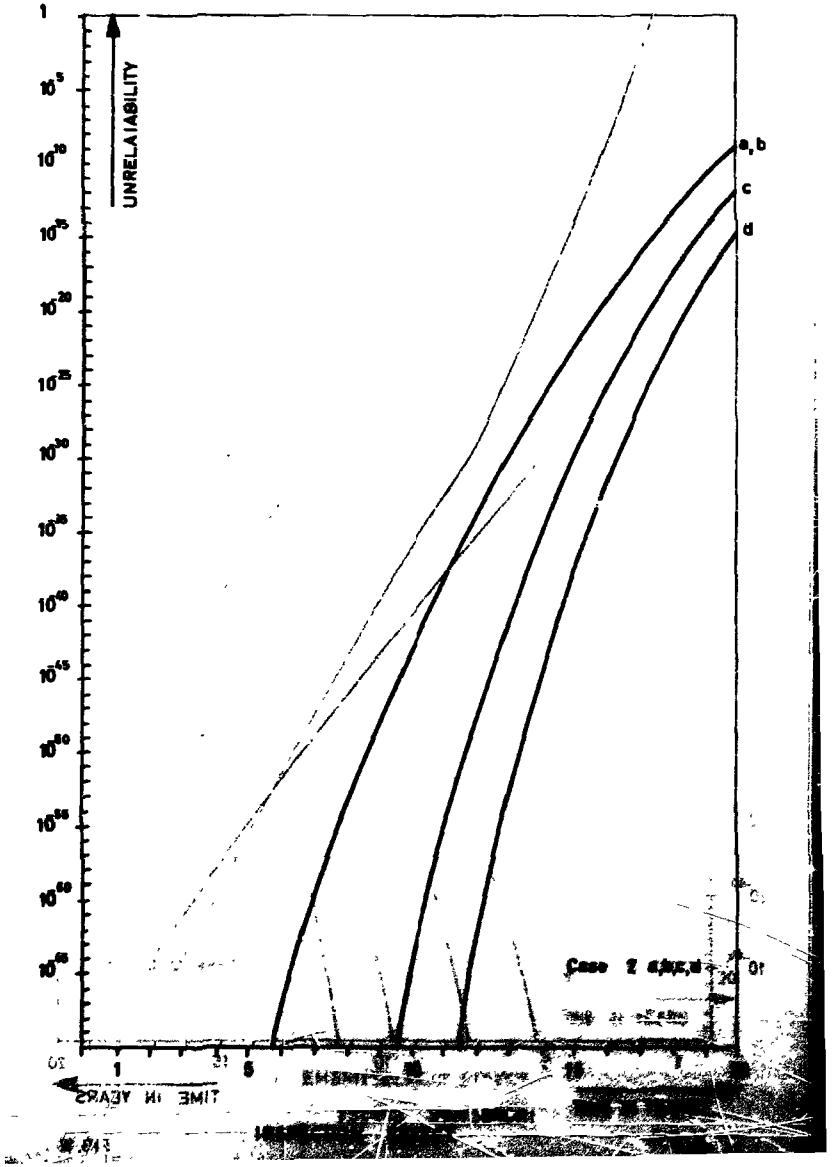
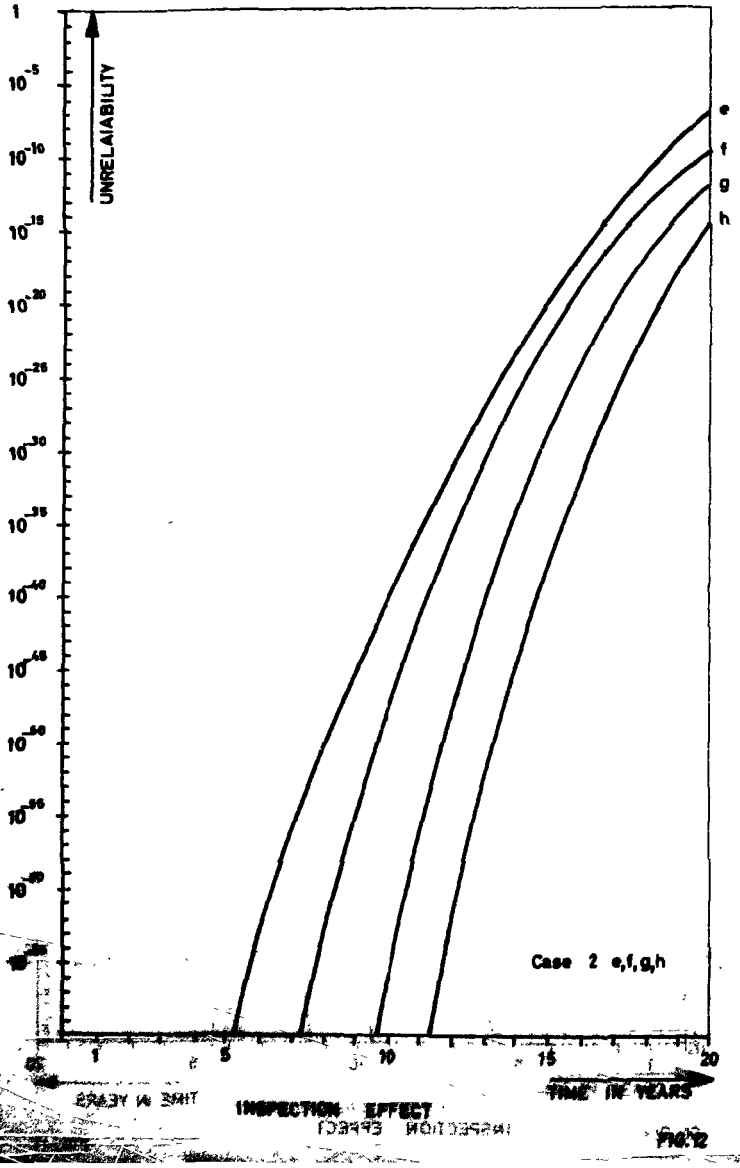

UNRELIABILITY
1
10^{-5}
10^{-10}
10^{-15}
10^{-20}
10^{-25}
10^{-30}
10^{-35}
10^{-40}
10^{-45}
10^{-50}
10^{-55}
10^{-60}
10^{-65}
$\alpha = 1/10$
$\alpha = 1/4$
$\alpha = 1/2$
$\alpha = 3/4$
Case n° 1
1
5
10
15
20
TIME IN YEARS
EMBRITTELMENT EFFECT

FIG. 8


UNRELIABILITY
10^{-5}
10^{-10}
10^{-15}
10^{-20}
10^{-25}
10^{-30}
10^{-35}
10^{-40}
10^{-45}
10^{-50}
10^{-55}
10^{-60}
10^{-65}
$\alpha = 1/10$
$\alpha = 1/4$
$\alpha = 1/2$
$\alpha = 3/4$
Case N° 2
1
5
10
TIME IN YEARS

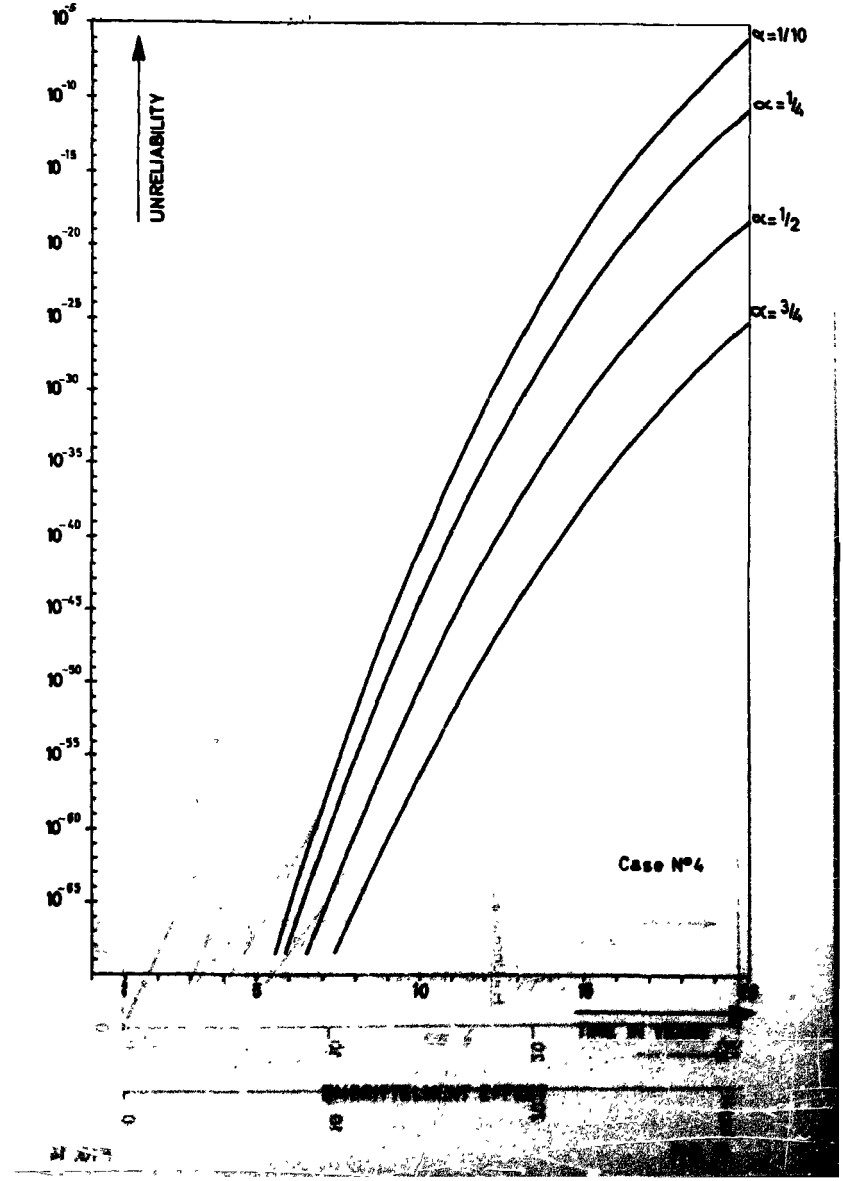

UNRELIABILITY
α=1/10
α=1/4
α=1/2
α=3/4
Case n° 3
TIME IN YEARS
ENRICHISSEMENT = EFFECT


UNRELIABILITY
1
10^{-5}
10^{-10}
10^{-15}
10^{-20}
10^{-25}
10^{-30}
10^{-35}
10^{-40}
10^{-45}
10^{-50}
10^{-55}
10^{-60}
10^{-65}
a, b
c
d
Case 2 a,b,c,d
TIME IN YEARS

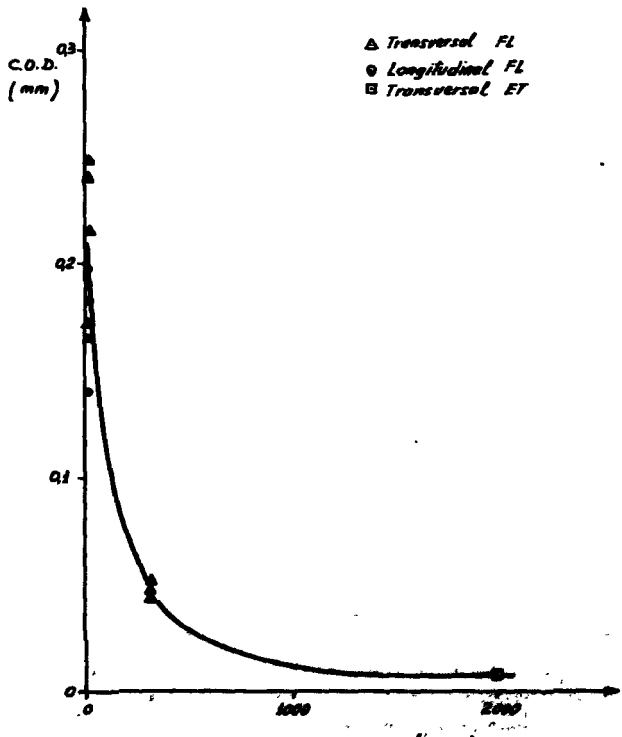


INSPECTION EFFECT

FIG. 12


UNRELIABILITY
α=1/10
α=1/4
α=1/2
α=3/4
Case N°4

Case n° 4
Case n° 1
Case n° 2
Case n° 3
H=Unreliability
ξ=Safety coefficient against fracture
20
10
1
0
0
1/10
1/4
1/2
3/4
1
α


C.O.D.
(mm)
0,3
0,2
0,1
0
1000
2000
HYDROGEN CONCENTRATION (ppm)
Transversal FL
Longitudinal FL
Transversal ET

A REVIEW OF THE SAFETY ASPECTS OF THE DESIGN OF PRESTRESSED CONCRETE PRESSURE VESSELS WITH REFERENCE TO LIMIT STATE DESIGN

C.W. Yu S. Gill

Existing Design Philosophy

The main safety consideration in the design of nuclear reactors has always been that of restricting the release of harmful fission products into the atmosphere. For this purpose, the primary containment of the fuel can and the secondary containment of the concrete pressure vessel itself, continue to represent the main precautions against disaster.

For the gas-cooled reactor, housed in a prestressed concrete pressure vessel, safety requirements in addition, have always demanded a restriction on the escape of gas from the steel-lined interior of the vessel, at least under test loadings.

The vessel loadings consist of the gas pressure, which is limited by relief valves, and the temperature load, which is limited by a secondary cooling system and insulation, and which can rise only slowly in the concrete due to the latter's thermal inertia.

It has been stated (1) that before gas leakage can be significant, the steel lining to the vessel must suffer widespread breaching, and that consequently structural failure of the main sections of the vessel only need to be considered where leakage is concerned.

Moreover a further assumption is usually made that all closures and penetrations of the concrete vessel maintain complete integrity.

Based upon these aims and assumptions, three design criteria have come to be adopted:

(1) that the elastic response of the structure should be such that under design load and test pressure, the stresses in the main sections of the vessel shall lie below permissible code values. This is the main classical design requirement for serviceability; the design of the steel lining is also, to a degree, dependent on a knowledge of the elastic response of the concrete.

(2) that there should be a mode of failure under overload conditions, such that deformations in the whole vessel are recognisably gradual and large before ultimate structural collapse.

(3) that there should be an adequate margin against ultimate failure; at the present time in Great Britain, it is required that the vessel barrel in the case of cylinders, should fail at a pressure not less that 2.5 times the design pressure, and that the end slabs should fail at a pressure not less that 3 times the design pressure.

In addition to these criteria for design, proof testing is normally carried out on completed vessels at a pressure 1.15 times the design pressure. The main purpose of this test remains that of indicating clearly that the vessel is adequately safe at design pressure, i.e. that it is not about to fail, and for this purpose, 1.15 seems a reasonable factor.

By the provision of instrumentation in the vessel, confirmation can be obtained during the test loading of the structure, that the design calculations forecast the actual behaviour reasonably accurately under service loadings. Such instrumentation can also confirm satisfactory behaviour during construction, commissioning and operation.

Other aspects which may be listed under the heading of existing safety philosophy are such items as inspection during construction and quality control of materials.

Results of model testing of prototypes also ensure that special arrangements of vessel geometry either of the whole structure or of parts of the structure, can be satisfactorily analysed.

Shortcomings of Existing Criteria

Although the three design criteria listed, may all be apparently satisfied by applications of acceptable analytical methods and arrangements of suitable vessel configurations, it should be realised that to a considerable extent, the overall safety of a prestressed concrete pressure vessel still depends on the integrity of many secondary layout details. For example all inserts and closures, and the insulation and cooling systems represent safety problems. These problems are not necessarily resolved by meeting the main criteria but by good planning and detailing, by controlled construction practice and by exemplary inspection. Each of these problems is usually given special ad hoc consideration.

It should also be realised that the assumptions and simplifications which have to be made in calculations may vary for different methods of analysis and for different layouts of vessel.

As for load factors or safety factors for any particular design condition, these should be specifically suitable for each configuration of vessel, although in the past similar factors have been used for very different layouts.

Moreover no realistic process yet exists for integrating into designs, proper allowances for time-dependent and temperature-dependent strains, in particular for thermal creep and for other secondary effects. Nor is it yet customary to allow in analysis for the involved stress histories of all concrete sections.

As the setting concrete generates heat of hydration, it expands and the stresses set up are relieved to a considerable extent by creep. Later the concrete having hardened, cools and contracts. The contraction stresses are tensile and increase the shrinkage stresses which begin to occur. Dead load stresses will load the concrete further and the extent to which all these stresses are dissipated and redistributed depends on the degree to which creep is still acting.

Undoubtedly there is an indeterminate condition of locked-in stress which represents a datum upon which are later imposed commissioning and operational stresses.

In addition the nature of the mechanical loading imposed on the pressure vessel concrete is cyclical, and in a realistic design, the effects of this repetitive loading on subsequent stress redistribution should be allowed for fully. It is in this sense that the concrete's stress history is of importance.

At first sight the three main design criteria, may appear reasonably satisfactory. However, an examination reveals a certain inconsistency and arbitrariness.

For example, on the one hand the designer is assured that relief valves will prevent the internal pressure from rising above a certain value, whilst on the other, he is required to spend a lot of his time examining modes of rupture under overload and ensuring that the [illegible] nor is it clear to what extent the effect of gas pressure penetrating between the lining and the concrete as clearance and leakage [illegible] relief valves.

In addition the designer refers [illegible] inertia but never satisfactorily [illegible] occurring in the concrete of operating vessels.

When it comes to the choice of overall load factor for the vessel, the values of 2.5 and 3 appear to have no real scientific basis; nor can it be established that by using these figures safety is fully guaranteed. Furthermore it cannot be claimed that the figures are the result of experience because none of the vessels built has yet had a service life long enough to permit any realistic statistical analysis, although the Foulness model tests (2) of the U.K.A.E.A. go some way towards remedying the situation.

The elastic analysis carried out has also been subjected to criticism in some quarters on the grounds that it is only the average working stresses that can be kept below permissible levels. It is frequently pointed out that the state of stress in certain parts of the structure does not neccessarily give a true picture of the overall serviceability.

It is evident that in order to be assured of a satisfactory design, the pressure vessel designer not only needs to know how safe the vessel is under overload conditions, but he also needs to know this at all stages and under all combinations of loading. Using the existing design criteria, he cannot certainly achieve these objectives.

However, if the limit state design concept is adopted, the safety of the structure can be systematically and logically assessed, provided the necessary data become available.

It should be pointed out that the ultimate load method of design, which is utilized for pressure vessels at the present time, in addition to the elastic analysis, is in itself one aspect of limit state design.

When the failure mechanism or mechanisms are known, the ultimate load method well represents the behaviour mode of the structure near collapse and consequently, satisfactory strength can be inferred, with confidence, at service load level. However, this aspect is only one of many that need consideration if the full limit state design method is adopted.

Limit State Design

Limit state design is now a well-established procedure widely applied to conventional structures, and which considers variations in both loading and material strengths from a statistical-probabilistic viewpoint. No apology need be made for re-stating those aspects of the theory relevant to the present thesis.

The governing equations for characteristic loads and strengths may be stated thus:

Characteristic load = mean load + (K_L x standard deviation)

and

Characteristic strength = mean strength − (K_m x standard deviation)

where K_L and K_m are factors with values which ensure respectively that the probabilities of the characteristic loads being exceeded and of the characteristic strengths not being achieved, are of a known, acceptable order.

Furthermore, the strength of the material in the finished structure may be weaker than that found from tests on samples. For example in the case of concrete this could be due to the inherent variability of the material as a result of its method of manufacture; the degree of compaction may not be the same on site as in laboratory samples; impurities may be present in site concrete and consequently its strength may be reduced. To allow for these factors which tend to weaken the strength of the material in the completed structure, a further partial safety factor is applied.

Thus, for the material;

$$\text{Design strength} = \frac{\text{characteristic strength}}{\gamma_m}$$

Similarly, the load applied to the structure or to part of it, may be greater than anticipated due to errors in design assumptions or errors in construction etc. Hence, for the loading;

$$\text{Design load} = \gamma_L \times \text{characteristic load.}$$

The choice of the magnitudes of γ_m and γ_L depends on how acceptable it is for these adverse effects to occur. Obviously the chosen values of γ_m and γ_L will determine the probability of these adverse effects happening.

For example, let us consider the strength of a section, which is governed by the compression strength of concrete. Assuming that all necessary data are available, the designer can select the appropriate values of K_L, K_m, γ_m and γ_L, which introduce the probabilities of occurrence P_m, P_L and P_m for the various circumstances, e.g. the probability that the design load will be in excess of the characteristic load is P_L, etc. The probability of the section collapsing is then $P_m \times P_L$. Similarly, the principal members of a structure are chosen so that ensure the probability of the whole structure reaching the collapse state can be calculated.

In general, a structure under service conditions, should not only carry the load safely, but it should also not deflect excessively and thus cause damage to interior finishings or installations. Partial safety factors and probabilities against the structure reaching an excessively deflected condition can also be estimated.

Finally, structural members should not be damaged locally by cracking and spalling of the concrete thus exposing the reinforcement to corrosion. In this case also, the probability of the structure reaching such a limit state can be assessed.

Thus for a structure to be satisfactory it has to be designed for several limit states.

A structure can be said to be well designed if it can be shown that the probebilities of each of the limit states being reached are constant and acceptable, provided of course that the resulting cost of the structure is realistic.

Theoretically, this is possible if all the statistical data are obtainable for assessing the probabilities p_f, p_m, P_f and P_m.

It should be accepted that identical probabilities cannot be arranged for all limit states applied to structures and particularly to the prestressed concrete pressure vessel because of the non-availability of certain data.

This problem may be overcome by accepting, in certain cases, a lower probability. For example, for those limit states, the attainment of which would result in serious loss of life or irreparable damage, or if the behaviour of the material and the variable nature of the loading were difficult to determine, then lower likelihoods of reaching such limit states may be designed into a scheme.

Such a step may be achieved by varying the partial load factors γ_m and γ_f for the different limit states. For example γ_f can be considered to be the product of γ_{f1} and γ_{f2} in which γ_{f1} caters for the variations of the loading in the structure as compared with its design load, and γ_{f2} depends on the severity of consequence when the limit state is reached. The theoretical values of γ_{f1} and γ_{f2} may be inadequate or invalid in some cases due to the lack of statistical data, and values should have to be chosen from experience and from observation of the behaviour of structures over a long period.

The product $\gamma_f.\gamma_m$ is known as the global factor of safety and can be

used as a measure of the factor of safety against a limit state being reached, thus giving a physical meaning to the analysis.

Application of Limit State Design to Prestressed Concrete Vessels

If it can be accepted that there is a need for reappraisal of the design philosophy of pressure vessels, it may be interesting to examine to what extent the limit state method can be a logical development.

For ordinary structures it is the practice to group limit states under the following headings: collapse, deformation and local damage, as explained above. In fact, it is possible to group all the possible service and failure limit states appropriate to a comprehensive concrete pressure vessel design, under one of these three categories. This can be done from a knowledge of the operating and functional requirements of the vessel.

Table 1 gives in general terms the operational procedures and functional requirements of a pressure vessel in their logical order.

TABLE 1

Constructional, Commissioning and Operational Procedures	Functional Requirement
Concrete Placing.	Satisfactory Compressive Strength. Satisfactory Density. Heat of hydration temperature recorded. Shrinkage joints and good curing to prevent shrinkage cracking.
Check foundation tilt.	Level of foundation checked to ensure core and vessel verticality to prevent inter alia, fuelling mechanism jamming.
Prestressing of Cables.	Satisfactory Steel and Concrete stresses before and after losses. (Security of anchorages. (Lift-off test - check to ensure adequate (residual tendon force.
Proof Testing with air.	Satisfactory Strains recorded. Satisfactory Overall vessel deformation particularly top cap. Lining Gastight. No cracking.
Hot run up to design temperatures and crossfall.	No cracking. Mainly intended to check insulation. Lining gastight.
Gas Pressure Applied.	Steel and concrete stresses acceptable. Deflections acceptable. No cracking.
Check cable stress.	Steel and concrete stresses acceptable.
Full commissioning.	Check that design stresses are realised in practice under working conditions and strains, [illegible] a [illegible]
Operational procedures and depressurisation and temperature rise and fall.	[illegible] magnitude and [illegible] compatible. [illegible] No cracking.

In general, by examining Table 1 the mode of behaviour of the vessel can be assessed under service conditions by postulating various limit states governed by factors arrived at from the statistical-probabilistic analysis. For example, the serviceability, the design load, and the test load limit states are characterised by mechanical loadings which are well-defined in their range, magnitude and frequency. In addition, various failure modes may be examined as limit states.

By this means, a preferred sequence of failure modes may be facilitated to promote the greatest safety. Not only would each failure mode be gradual where this was possible, but the preferred sequence would ensure that the least serious failure would be likely to occur earliest.

These safety considerations assume paramount importance when new nuclear reactors are located adjacent to large conurbations with the objective of economising in transmission costs.

For example, for a cylindrical vessel the suggested sequence of limit states might be

1) Limit state corresponding to working load for temperature and pressure.
2) Limit state corresponding to design load for temperature and pressure.
3) Limit state corresponding to test loading for temperature and pressure.
4) Temperature limit state corresponding to breakdown of cooling system and/or insulation.
5) Limit state corresponding to relief valve control pressure.
6) Local first cracking of concrete.
7) Loss of stiffness due to extensive cracking in the barrel.
8) Steel lining rupture.
9) Radial cracking in end cap.
10) Barrel, hoop tension failure.
11) Shear failure in end cap.
12) Bending failure at end cap/wall connection.
13) Prestressing cable rupture.

The critical stress or strain criteria controlling each of these limit states can then be investigated in the manner illustrated by Baker (3).

If the sequence of limit states listed is accepted as a basis for the design of a prestressed concrete pressure vessel, values for partial and overall safety factors for the various states, can also be assigned in a manner similar to that suggested by Baker in Table I of his paper.

The partial factors suggested in Baker's example are such that for later undesirable limit states, a low probability of their occurring is arranged. Where stress and strain at a limit state are difficult to assess precisely, a low probability of these states being reached is again arranged.

It is evident that with the existing design philosophy, for all of the listed states to be catered for, it would involve the vessel being over-designed in some sections.

Difficulties in Applying Limit State Design to Prestressed Concrete Vessels

As indicated by Baker, the partial factors suggested in his example are for illustrative purposes only, because in many cases, data distribution frequency and characteristic loads (particularly those resulting from temperature) are lacking at present. Because of this lack of data some of the partial safety factors may appear excessively high. However his table does indicate the principles involved and the logic of the approach. When more nuclear power stations have been built and more extensive instrumentation has been installed, more of the necessary data should become available.

In the case of pressure vessel limit states affected by thermal creep, in addition to the lack of data already discussed, there are other difficulties.

Consider the limit state of local cracking due to shear. Since in this case stress is the criterion, either the characteristic compressive or characteristic tensile strength may be used. However the probability and global safety calculated in the usual manner are not likely to be the appropriate values, because shear cracking strength is not directly proportional to either the compressive or tensile strength of concrete, but depends on many other factors. Therefore it will be necessary either to introduce a third partial safety factor to cater for this, similar to the Russian practice in ultimate strength design (4) or the partial factor selected for the load must allow for the shear affect. In either case, appropriate statistical data will be necessary.

When a limit state involving stress affected by creep and shrinkage at elevated temperature is being considered, the creep data to be used in the analysis may be obtained from control specimens. Again if the global safety factor and probability are calculated in the usual manner, they may not be the true values. This is because "characteristic creep" is not directly proportional to concrete compressive strength. Furthermore, the method of creep analysis would influence the stress values obtained in this case. It would therefore be necessary to introduce a third partial factor unless an allowance could be made in this respect in selecting the appropriate [illegible] creep value or the strength and loading [illegible]

Take a further example and consider the experimental work carried out at Imperial College and The City University, London, on the behaviour of the perforated end slab of a pressure vessel subjected to radial pressure and temperature load. Fig. 1 shows the stress history at the periphery of the perforated region (5). T_4 indicates the stage at which the pressure load was reduced after 100 days. The calculated locked-in field stress was 2.2 $MN/m2$ causing a tensile hoop stress of 3.2 $MN/m2$ thus cracking the slab radially. If this particular cracking limit state is under consideration, then it is evident from the process of analysis that the relationship between the resultant tensile stress and the creep rate is complex. Calculations for this limit state based on the concrete's compressive strength in any way would be misleading.

The above three examples are intended to indicate the difficulty of applying the limit state design concept in certain instances due to lack of data. Nevertheless the principle can be seen to be a logical one if the aim is to achieve the greatest safety in pressure vessel design without using unnecessarily high safety factors.

Conclusions:

1. Prestressed concrete pressure vessel designers should seriously consider the limit state design concept since it enables every critical part of the vessel, under all loading conditions to be logically considered. The probability of failure can be assessed and a preferred sequence of limit states arranged, in order to give the greatest safety for a given pressure vessel.

2. However, in order to apply this principle to design in practice, more data will be necessary. The data required, such as the pressure distribution, the temperature distribution, the frequency, likelihood and effects of pressure and temperatures surges and the way in which construction, commissioning and operating procedures affect design parameters, should be collected from existing vessels and from instrumentation on future vessels.

3. A critical study of the appropriate parameters to be used at the various limit states must be carried out to enable correct global factors to be assessed.

References:

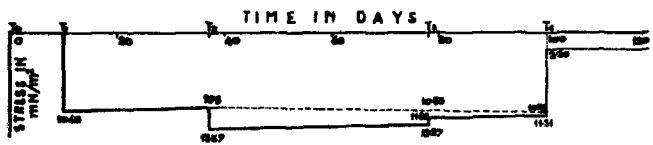
1. N. T. Barrett and I. Davidson, "Design Philosophy and Safety". Proceedings, Conference on Prestressed Concrete Pressure Vessels. Institution of Civil Engineers 1968. pp. 65 - 72.

2. I. Davidson and A. C. Purdie, "Small-scale P.C.P.V. tests at Foulness". Paper No. 7. Conference on Model Techniques for P.C.P.V. July 1969.

3. Baker, A. L. L. "Safety of Pressure Vessels". Proceedings, Conference on Prestressed Concrete Pressure Vessels. Institution of Civil Engineers 1968. pp. 79 - 84.

4. Yu, C. W., Corbin M. and Hognestad, E. "Reinforced Concrete Design in the U.S.S.R.". Journal of the American Concrete Institute. Vol. 31, No.1, July 1959.

5. Stefanou, G. D., Yu, C. W. and Gill S. "An experimental Investigation into the Behaviour of Perforated End Slabs for Concrete Pressure Vessels under Temperature and External Load". Symposium on Model Techniques for Prestressed Concrete Pressure Vessels. The British Nuclear Energy Society, July 1969.



STRESS DIAGRAM

FIG. 1

For Presentation at the 3d CREST Meeting of Specialists on the Reliability of Mechanical Components and Systems for Nuclear Reactor Safety

Risø, Denmark, September 24-26, 1969

Analysis of a German Pressure Vessel and Boiler Drum Statistics

by

G. Mieze

Institut für Reaktorsicherheit
der Technischen Überwachungs-
Vereine e.V.

Köln, Germany

Abstract

The pressure vessel statistics are set out by the Vereinigung der Technischen Überwachungs-Vereine (VdTÜV) and are contributed by all Technischen Überwachungs-Vereine (TÜV). A description of the characteristics of the statistics is given and the VdTÜV failure reports are explained. Furthermore, the analysis of the primary data and the determination of failure rates is shown.

The boiler drum statistics cover most of the boiler drums operated in the Federal Republic of Germany. Once more a description of the characteristics of the statistics is given. In addition, the observed failure modes are reviewed. Furthermore the analysis of the primary data and the determination of failure rates is discussed.

The failure rate figures obtained from the VdTÜV statistics have provided us with an idea of the order of the failure rate connected with reactor pressure vessels, while the failure rate data derived from the boiler drums statistics is suggested to be more realistic in connection with nuclear pressure vessels. The relevance of the data to nuclear pressure vessels is discussed.

Analysis of a German Pressure Vessel and Boiler Drum Statistics

1. Introduction

Much effort has been spend in the development of the reliability analysis technique. But the absence of appropriate input data became obvious, especially of pressure vessel data. So we decided to analyse the material already collected in Germany. A study of the reliability of conventional pressure vessels has been initiated. Our objective has been to obtain more accurate and realistic data on thickwalled pressure vessels which would enable us to extrapolate to nuclear pressure vessels failure behaviour. The first step of that study is concerned with conventional pressure vessels and has given us a knowledge of the order of magnitude of the failure rate data. This step has been completed. /1/

An analysis of the results obtained and an analysis of the material left for investigation, lead to a second step which is concerned with boiler drums. The boiler drums investigated are comparable with reactor pressure vessels in overall dimension, wall-thickness, design pressure and temperature. So the results of this step will be more representative for nuclear pressure vessels than those of the first step.

This paper reports on the technique used in the analysis as well as on the results and its consequences.

2.0 Pressure Vessel Statistics

2.1 Design of Statistics

The data analysed are taken from the VdTÜV Statistics /1/. This statistics includes all failures from vessels which must be inspected in compliance with official regulations. Deficiencies are not reported. By definition a failure is defined to have occured, when the vessel had to be repaired or replaced. Vessel failures are reported by authorized inspectors on a form shown in Fig. 1. The number of vessels in operation as well as the entries and deductions are taken from an annual statistics of the Technischen Überwachungs-Vereine (TÜV) /2/. A classification of the vessels according to operating conditions, design etc. is not possible.

2.2 Analysis of Primary Data

The material shortly described in the preceding paragraph has been analysed and the following data are obtained.
The total number of vessels, which are in operation per year, have been taken from /2/. The corresponding data from 1953 and 1954 have been estimated from the graph of the data.
Also the number of vessels operational have been taken from /2/ according to its year of manufacture. The error due to new commissioning of old vessels is below 1%. Again the numbers from 1953 and 1954 are estimated from a graph of the data.
The number of pressure vessels which have failed per year classified according to their year of manufacture are taken directly from the form described in the preceding paragraph. All data described are available for the years 1952 until 1967 respectivly.

2.3 Determination of Failure Rates

The failure rate of the pressure vessels is calculated in accordance with the German standard DIN 40041 /3/. See also /4/.

$$q\ (\Delta t_i,\ t_i) = \frac{B\ (t_i) - B\ (t_{i+1})}{B\ (t_i)\ \Delta t_i} \qquad (1)$$

Where is:

$q\ (\Delta t_i,\ t_i)$	-	statistical estimate of the failure rate
$B\ (t_i)$	-	number of components operational at the time t_i
$B\ (t_{i+1})$	-	number of components operational at the time t_{i+1}
Δt_i	-	time intervall $(t_i,\ t_{i+1})$.

In all, 15 samples were taken, namely the pressure vessels which have been manufactured per year beginning 1952 up to 1966. A time intervall $\Delta t = 10^5$ hours has been used.
The estimates are shown in Fig. 2

The failure rate is then estimated from the data obtained from eq. (1). We have tried the data in several probability papers. The best fit appears to be the Weibull-distribution. Two methods have been applied.

1. The failure rate is estimated using the data of eq. (1), see Fig. 2
2. The reliability function R (t) is estimated using the cumulative frequency. From the reliability function then the failure rate is obtained. See Fig. 3.

We have used both procedures and compared the results obtained. The equations used are as follows.

$$R(t) = e^{-\alpha t^{\beta}} \qquad (2)$$

where R(t) is the reliability function and t the problem time. From this the failure rate is derived:

$$Z(t) = \alpha\beta t^{\beta-1} \qquad (3)$$

The values of the parameters α and β obtained from the data analysed are

$$\alpha = 1{,}49 \cdot 10^{-5}$$
$$\beta = 0{,}43$$

As will be empasized in the following discussion, the reference data contain some inaccuracy, the magnitude and consequence of which is hard to estimate. Taking this into account, the results are to be considered with some reservation. Quick and generalising conclusions, especially concerning reactor pressure vessels, should be avoided.

2.4 Discussion

All pressure vessels having a pressure volume product $p \cdot V \geq 1000$ at[x] m^3 at[x] require inspection, independent from their design and operating circumstances, but having a pressure of $\geq 0{,}5$ at[x]. These pressure vessels are manufactured from various materials, e.g. copper, cast iron, steel, they have various dimensions from 0,5 up to several metres and are used for different purposes, e.g. for storage of chemicals, such as steam, heated rolls

x) at[x] = atmosphere overpressure

in paper mills, or as condenser vessels, heat exchangers, spray coolers in a power plant etc. They are operated over a wide range of temperatures and pressures (0,5 to more than 1000 atü) due to their various applications. The following causes for failure of the vessels have been found:

design and manufacturing deficiencies,
poor construction,
operating and environmental influence,
wrong operation (to a large extent human error),
corrosion and aging and
pressure testing.

The failure modes are as follows:

Sudden total destruction during operation, the original function of the vessel being disturbed and internal and external testing by the inspecting organisations.

The authorised inspectors have to decide whether it is a failure or a deficiency, an exact definition of both is not given. So the decision of the inspector, who has to fill in the form (Fig. 1), as to wether it is a failure or deficiency is also influenced by the amount of work he has to carry out. According to our information the tendency to report all failures has increased over the last year. Nevertheless the number of reported failures per year remained almost constant, although the number of vessels increased six-fold since 1952.

One of the reasons may be improved quality of the new vessels. Manufacturing methods, materials, welding procedures and the construction have undergone a very favourable development during the last decade. But there is some doubt that this influence is solely responsible for the decreasing failure frequency. It is assumed that failures, which have occured, had not been reported. By putting in force the new regulations /5/ in 1958, which had already been applied in 1956 and 1957, as they were already available in form of a draft - the failure behaviour of the pressure vessels was distorted due to the higher failure frequency caused by the pressure test according to /5/.

Due to the lack of data, with regards to the number of vessels in service, to entries and deductions in 1953 and 1954, these were extrapolated from the data gained in the other years. The failure rate has been calculated using the entries of 1952 - 1957 as the sample size, respectivly. By this method an error was introduced due to the fact that some old pressure vessels had been taken back into service. This error should be below 1%.

The widely scattered estimates of failure rate q, as shown in Fig. 2, is caused by an increase of pressure vessel entries at approximately constant failure frequency. The resulting failure rates of the various samples are decreasing with the advancing years of manufacture. This effect is responsible for the exagerated value of the calculated deviations.
The estimates of the failure rate are larger than previously for the time intervall between 8 and 9×10^4 service hours, but the assumption of an increasing failure rate (failure by aging) is misleading. We don't believe, that the failure rate is actually increasing at this stage. This effect is probably due to insufficient data.
The values of the cumulative frequencies in Fig. 3 are also scattered as a result of an increasing number of pressure vessels at approximately constant failure frequency. In addition one observes an accumulation of failures at rounded-off hours of service, especially at service times exceeding 1000 hours. Our conclusion is that usually rounded-off hours of service time are given, or are estimated according to the type of service.

The function Z(t) in Fig. 2 has been smothly drawn trough the modes of the estimate of the failure rate in the respective time periods. The straight line in Fig. 3 is also drawn trough the modes. The modes were estimated. A calculation of the modes would not give more exact results, due to the lack of suffucient data for each time period. Theoretically a displacement of the points should be possible. But this deplacement would only slightly change the parameter α, the slope of the straight line would remain constant and thus the parameter β.

3. Boiler Drum Statistics

3.1 Basis of Statistics

In 1961 a study was initiated which includes all high pressure steam drums operated in the Federal Republic of Germany and which are supervised by the TÜV and the organisations which operate the boilers. All essential data of the intact drums as well as drums with faults are entered in a special form. 241 drums, including 33 drums with faults are investigated. The drums are operated at a pressure ranging from 60 to 140 atü and temperatures of 290 - 350 °C and are made from high-temperature structural steel of different compositions. The operating times of the drums are of very different length as the years of commissioning vary from 1929 to 1958. The faults observed were corrosion marks and cracks of different size.

3.2 Determination of Failure Rates

Again the failure rates may be calculated using the two methods described in chapter 2.3. But some modifications are necessary due to the kind of data analysed.

1. The actual time at which the faults are developed is not known as all the faults were discovered during internal inspections to be performed at a three years intervall. So a negative deviation of the time at which the faults are developed of three years is introduced.

2. The operating times of the boiler drums are nearless equally distributed along a period of time up to $1{,}5 \cdot 10^5$ hours. So eq. (1) must be modified taking into account the different operating times. This also applies to the calculation of the cumulative frequency distribution.

The calculation of the probability distribution and its parameters proceeds along the following items: The cumulative frequency distribution is calculated and a deviation of minus three years is assigned to the time of internal investigation which revealed a fault. These data are tried in several probability papers to find out the type of distribution. Then the best fitting curve along these data points is used to calculate the parameters of the probability distribution.

The cumulative frequency is calculated by

$$A(t_i, t_o) = \sum_{i=1}^{m} \frac{1}{B(t_o) - \sum_{j=1}^{i} n_j} \qquad (4)$$

where m designates the number of faults, $B(t_o)$ the number of vessels intact at time $t=t_o$, n_j the number of vessels which have to be taken out of the statistics in intervall of time j due to the end of operating time and $A(t_i, to)$ is the cumulative frequency of faults at operating time t_i.

The best fit of the data points was again found to be the Weibull-distribution. The analysis is made first for all boiler drums, then for the CuNi-drums only and finally for the drums whithout the CuNi-drums. This was suggested by the discovery of faults at 20 drums out of a sample of 46 CuNi-drums. For more details see /6/ and /7/.

The sample of all boiler drums contained 241 items of which 33 showed faults. A catastrophic failure has not been observed. The parameters of the Weibull-distribution, eq. (3), are calculated to be

$$\beta = 1.73$$
$$\alpha = 6,07 \cdot 10^{-10}$$

The sample of the CuNi-alloy made boiler drums contained 46 items of which 20 showed faults. The Weibull-parameters obtained are

$$\beta = 2,7$$
$$\alpha = 7,36 \cdot 10^{-14}.$$

The sample of boiler drums without the CuNi-alloy made ones contained 195 items of which 13 showed faults. The Weibull-parameter calculated from these data are

$$\beta = 2,7$$
$$\alpha = 2,84 \cdot 10^{-17}$$

The results are given in Fig. 4 to Fig. 7.

Although the data analysed are more accurate and more complete from the statistical point of view than those of the pressure vessel statistics again

the relevance of the data obtained to reactor vessels is restricted. Therefore the data should be handled with care when applied to reactor pressure vessels. This will be explained in the following chapter.

3.3 Discussion

The statistical data analysed are in our opinion a complete set of information on the boiler drums operated in FRG. The limited accuracy of these data, however, should be borne in mind.
The data on operating times are very often estimated. Due to this fact an error is introduced in the failure rate parameters. Additionally, the faults always are discovered at internal investigations which have a three years intervall. So the actual time of failure can be off by as much as three years of calender time. This additionally, introduces an error. The failure rate of the boiler drums developing faults as corrosion holes and cracks thus should be used with care. However, the starting point of the failure rate, e.g. at time t = 0 can be obtained by considering the failure mechanics. The cracks as well the corrosion marks develop as the time goes on. So the possibility that a drum with faults is found immediately after the first start-up does not exist. This suggests a failure rate at time t = 0 of Z(0) = 0. Z(t) increased as the time goes on. The slope of the curve, however, strongly depends on the material emploid. So we decided to distinguish between the drums made of the CuNi-alloys and the rest of the drums. The analysis showed a marked difference in failure rates of the two groups of material considered. Our conclusion on this is that only the curves of the CuNi-alloy made drums, see Fig. 5, and the rest of the drums, see Fig. 6, give fairly accurate data respectivly, while the overall curve, see Fig. 4, does not apply to the data analysed.

Among the boiler drums no serious, catastrophic failure has been observed. Nevertheless an estimate of a failure rate for this type of failure would be most interesting. The following set of assumptions, however, might present an upper boundary approach to that number.

1. All of the 241 boiler drums have accumulated the same operating time which is supposed to be an average of the actual operating times. This gives an operating time of $8 \cdot 10^4$ hours.
2. An exponential failure distribution is assumed.
3. One catastrophic failure is assumed to occur at a operating time of $8 \cdot 10^4$ hours.

From those assumptions we obtain a failure rate of

$$z = 5 \cdot 10^{-8} \cdot h^{-1}$$

This estimate of course gives an upper limit of the actual failure rate.

4. Conclusions

As already emphasized in chapter 2.4 the failure rate of the pressure vessels analysed has been calculated from 15 samples with various running times and represents an average of all samples. The samples drawn contain pressure vessels of all types and varying conditions of operation and environment. The failure modes were: catastrophic failure of the vessel, e.g. either circumferential or langitudinal crack, leakage by smaller cracks, corrosion, failure of closures and failure of the vessel due to pressure test. So the failure rate obtained is not representative for reactor pressure vessels. However, the result certainly gives a knowledge of the upper limit of the failure rate of reactor pressure vessels.

More representative results are obtained from the boiler drums statistics. But nevertheless, it is hard to extrapolate from the behaviour of the boiler drums to the fault behaviour of reactor pressure vessels. The following differences should be borne in mind when the numbers of this report are applied to reactor pressure vessels:

Design

Reactor pressure vessels and boiler drums are designed according to different rules, for example the different ASME codes. Additionally, the reactor pressure vessels are penetrated by a few big nozzles while the boiler drums have a large number of small holes for the boiler tubing.

Material

Reactor pressure vessels must not be built using ordinary boiler steel. Compositions including elements which will be activated to radioisotopes having a long half-live period are not used for reactor pressure vessels. Additionally, reactor pressure vessels are plated by an austenitic material. So corrosion as observed in the boiler drums will probably not occur in reactor pressure vessels.

Manufacture

Again the boiler drums and nuclear pressure vessels are manufactured and tested according to different rules. As recurring internal inspections of nuclear pressure vessels are very difficult, often impossible, the manufacture and testing of these vessels is performed more careful than the manufacture of boiler drums.

Operating condition

The temperature and pressure conditions are almost the same for both the nuclear pressure vessels and the boiler drums. However, the number of start up and shut down procedures for boiler drums usually is much higher than for nuclear pressure vessels. On the other hand the neutron embrittlement of the reactor vessel material is unfavourable for the reactor pressure vessel. All these differences may influence the failure behaviour of nuclear pressure vessels to a large but unknown extent.
Due to the fact that all deficiencies of the boiler drums were discovered at internal inspections and so catastrophic failures were prevented, the importance

of internal and external inspections of reactor pressure vessels is supported. This is emphazised by the fact that cracks of a length up to 2 m and depth up to 15 mm could develop in a time period of at most three years in boiler drums, while current reactor pressure vessels are designed for a lifetime up to 40 years without inspection. Proposals already are made /8/. Consequent external and internal inspections as well as pressure tests might improve the reliability of reactor pressure vessels some orders of magnitude.

Köln, den 10. September 1969
mi/go

/1/ G. Slopianka and G. Mieze, Failure Rates of Pressure Vessels, Part 1, Evaluation of VdTÜV Statistics
IRS - I 34 (1968)

/2/ VdTÜV, Jahresbericht der Technischen Überwachungs-Vereine e.V.

/3/ Zuverlässigkeit elektrischer Bauelemente, Begriffe
DIN 40041

/4/ Igor Bazovsky, Reliability Theory and Practice
Prentice Hall

/5/ Hauptverband der Gewerblichen Berufsgenossenschaften, Sammlung der Unfallverhütungsvorschriften, Carl Heymanns Verlag, Köln

/6/ K. Kußmaul, Beobachtungen an hochleistungs-Kesseltrommeln, VGB-Mitteilungen, 49. Jahrgang, Heft 2, April 1969, Seite 113 - 122

/7/ G. Slopianka, Ausfallraten von Druckbehältern, Teil III, Zuverlässigkeit und Ausfallraten von Hochdruck-Kesseltrommeln
IRS - I 37 (1969) (draft)

/8/ O. Kellermann, Dr. A. Tietze, Recurring Inspections of Nuclear Reactor Steel Pressure Vessels
Technical Report IAEA - 109, p. 1 - 16

Berichtende Stelle:	VdTÜV-Schadensliste Nr.

Schadensbericht

Druckbehälter

ausgestellt am ... in ... Ausfertigungen. Ausfertigung Nr. ...

I. Allgemeines

1. Tag und Stunde des Schadenseintritts: ...
2. Name und Wohnort des Betreibers: ...
3. Art des Betriebes: ...

II. Kennzeichen des Druckbehälters

1. Hersteller: ...
2. Fabrik-Nr. ... 3. Baujahr: ...

		Raum:		
4. Inhalt V	ltr			
5. Höchstzul. Betriebsdruck p	atü			
6. Höchstzul. Betriebstemp. t	°C			

7. Produkt $V \times p$: ...

III. Bauart (Zeichnung oder Skizze mit Hauptmaßen beigefügt):

1. Werkstoff: ...
2. Beschreibung (Herstellung, Ausrüstung, Verschlüsse): ...

IV. Betriebsverhältnisse

1. Verwendungszweck (Beschreibung des Arbeitsverfahrens): ...
2. Beheizung: ...
3. Druckmittel: ... 4. Druckerzeugung durch: ...
5. Beschickung: ... Eigenschaften des Beschickungsgutes (Korrosions-, Explosionsgefahr und dgl.): ...
6. Betriebsdauer: täglich ... Stunden Gesamtbetriebszeit etwa ... Stunden.

V. Überwachung

1. Vorgenommene Prüfungen: Dampfprüfung (Inbetriebsetzungsprüfung) am: ...
   Druckprobe am: ... Abnahmeprüfung am: ...
   Letzte (regelm. o.ä.) Untersuchung am: ... / mit ...
2. Hinweise auf Mängel: Die bei der letzten Untersuchung festgestellten Mängel wurden in der vorgeschriebenen Frist bis ... behoben.

VI. Betriebsverhältnisse (unmittelbar vor dem Eintritt des Schadens):

VII. Angaben über den Schadensumfang

1. Schäden an dem Gefäß und seinen Einrichtungen:

2. Schäden an Betriebseinrichtungen und Gebäuden:

3. Personenschaden: Tote[1]) Schwerverletzte: Leichtverletzte:

VIII. Wahrscheinliche Schadensursache

IX. Maßnahmen

1. zur Beseitigung des Schadens:

2. zur Beseitigung der Schadensursache:

X. Bemerkungen

XI. Ist gewerbepolizeiliche Untersuchung eingeleitet?

XII. Anlagen:

, den 19

Der Sachverständige:

[1]) Personen, die innerhalb von 30 Tagen nach dem Unfall verstorben sind, sind als Tote anzugeben.

FIG. 1 Continued

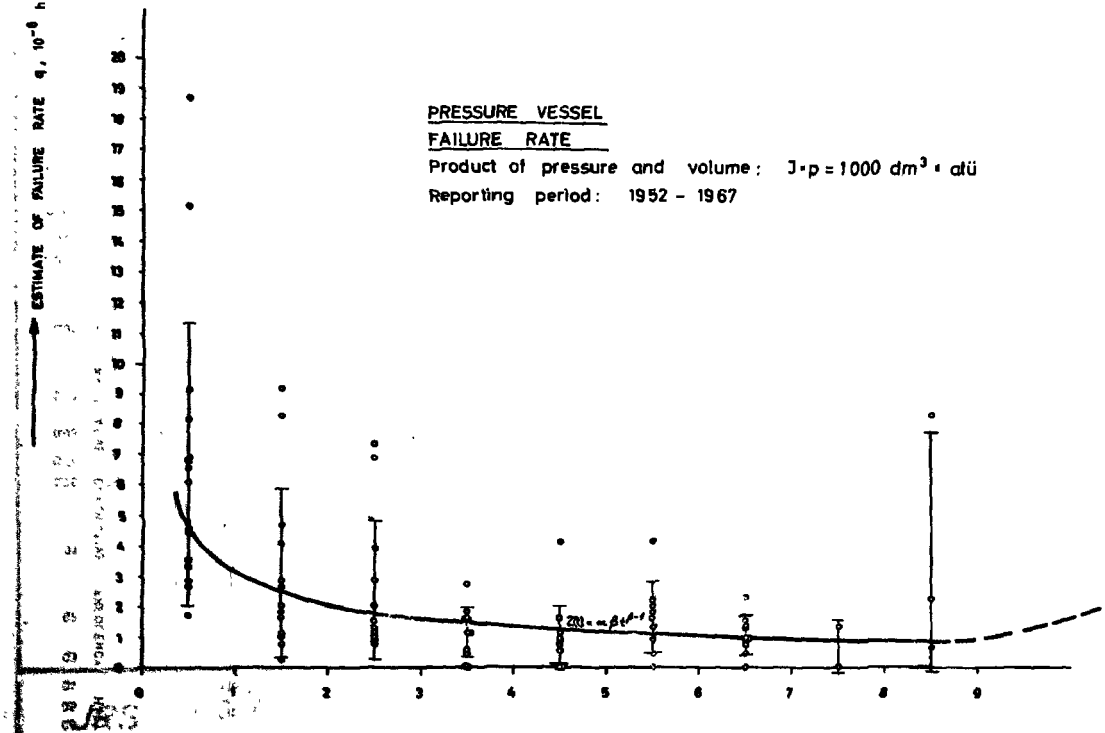

PRESSURE VESSEL
FAILURE RATE
Product of pressure and volume: J=p = 1000 dm³ · atü
Reporting period: 1952 – 1967
ESTIMATE OF FAILURE RATE q, 10⁻⁴ h
TIME INTERVAL Δt, 10⁴ hrs
0
1
2
3
4
5
6
7
8
9

FIG. 2

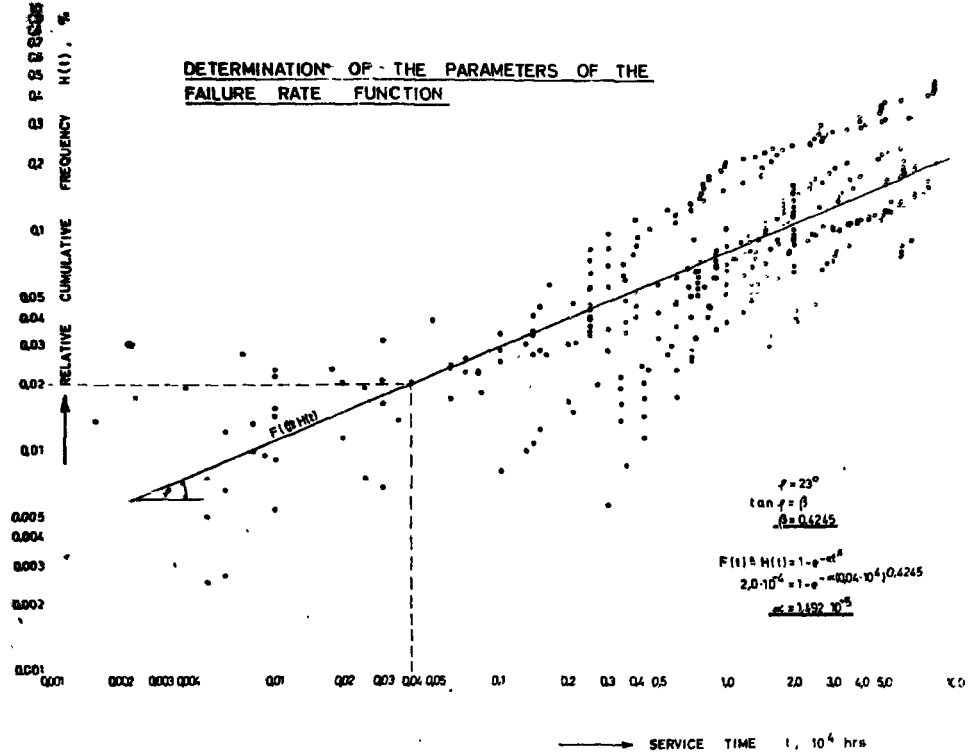

DETERMINATION OF THE PARAMETERS OF THE FAILURE RATE FUNCTION
RELATIVE CUMULATIVE FREQUENCY H(t), %
F(t)≙H(t)
SERVICE TIME t, 10⁴ hrs
φ = 23°
tan φ = β
β = 0,4245
F(t) ≙ H(t) = 1 - e^(-αt^β)
2,0·10⁻⁴ = 1 - e^(-α(0,04·10⁴)^0,4245)
α = 1,692 10⁻⁵

FIG. 3

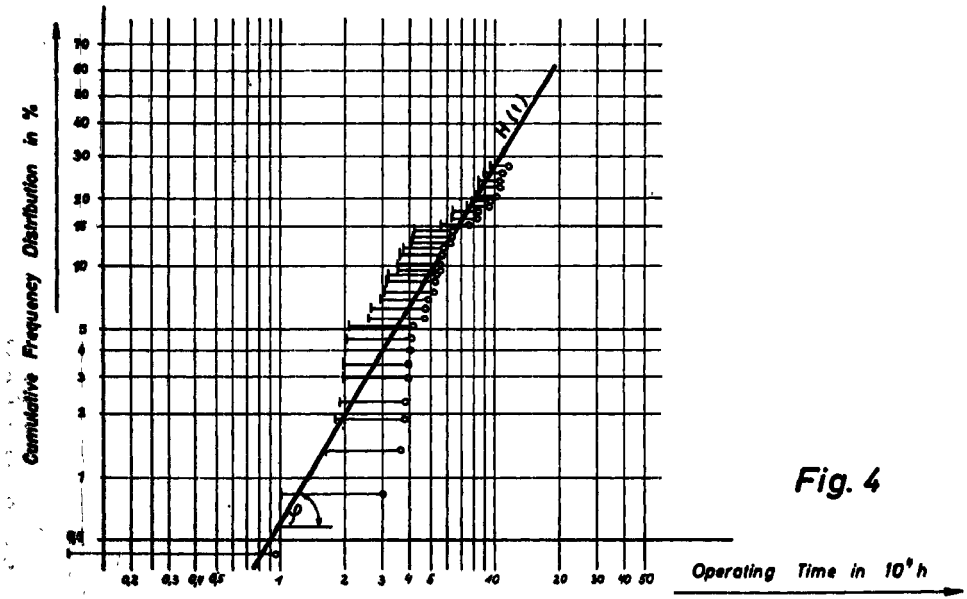
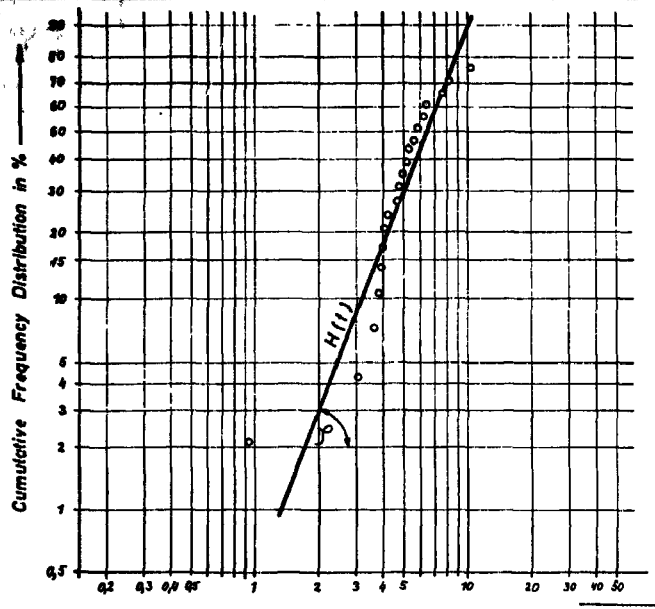


Fig. 4

IRS	Cumulative Frequency Distribution H(t) All Boiler Drums	134



$\varphi = 69{,}7°$

$\tan \varphi = \beta$

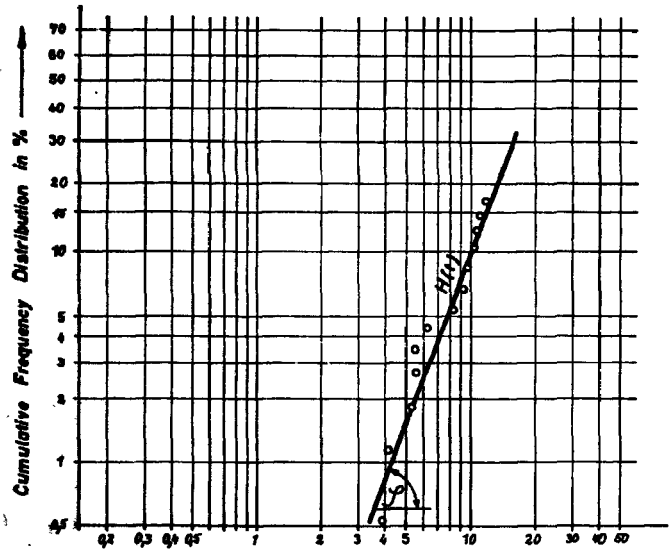
$\beta = 2{,}7$

$H(t) = 1 - e^{-\alpha t^{\beta}}$

$\alpha = 0{,}7363 \cdot 10^{-13}$

Fig. 5

JRS	Cumulative Frequency Distribution H(t) Cu Ni - Boiler Drums	135



$\varphi = 69{,}7°$

$\tan \varphi = \beta$

$\beta = 2{,}7$

$H(t) = 1 - e^{-\alpha t^{\beta}}$

$\alpha = 0{,}2641 \cdot 10^{-16}$

Fig. 6

JRS	Cumulative Frequency Distribution H(t) Boiler Drums exept the Cu Ni - Drums	136

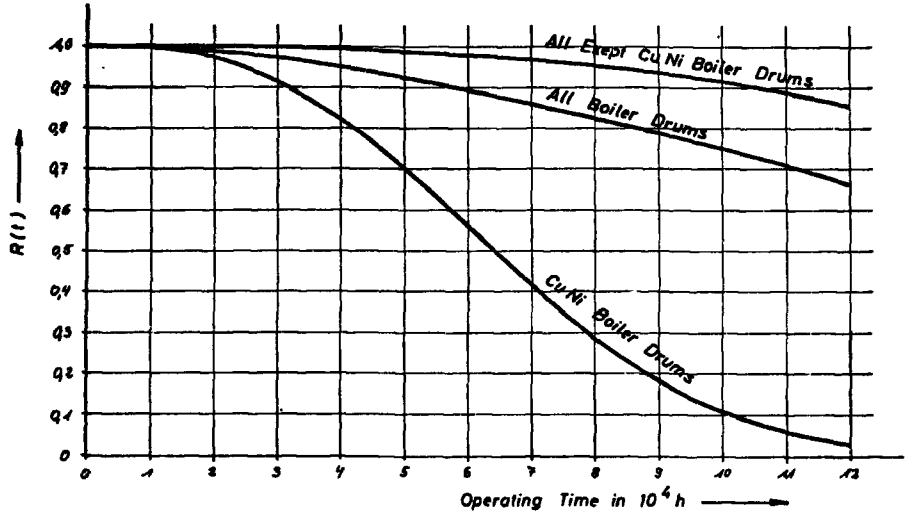


Fig. 7

JRS	Probability Function R(t) of Boiler Drum Groups	137

A SURVEY OF PRESSURE VESSELS BUILT TO A HIGH STANDARD OF CONSTRUCTION

By

C.A.G. Phillips, B.Sc.(Eng.),C.Eng.,M.I.E.E., United Kingdom Atomic Energy Authority, Health & Safety Branch, and R. G. Warwick, M.A., C.Eng., M.I.Mech.E., Associated Offices Technical Committee.

In view of the limited experience with nuclear pressure vessels, the United Kingdom Atomic Energy Authority, Health & Safety Branch, approached the Associated Offices Technical Committee when it was desired to arrive at the figures for the probability of failure of nuclear vessels with a view to establishing failure rates over a large sample of conventional pressure vessels built to similar standards. In the United Kingdom all steam boilers and a proportion of pressure vessels must be thoroughly inspected at intervals of about 1 year or 2 years to comply with the regulations laid down in the Factories' Act. These inspections normally consist of a visual examination of the boiler or vessel both externally and internally and are supplemented by more detailed examinations such as ultrasonic testing, radiography, magnetic or dye penetrant flaw detection, tube sampling, hydraulic tests, etc., as may be considered necessary by the competent person carrying out the examinations. It is the normal practice for these inspections to be carried out by specialist Engineering Insurance and Inspection Companies. Five of the major companies carrying out this type of work form the A.O.T.C. and it is from their records that this study is made and the initial phase fully reported elsewhere. (1)

In addition to carrying out inspections of boilers and pressure vessels during service, the A.O.T.C. Members carry out inspections of boilers and pressure vessels during construction and a separate study was carried out relating to this aspect.

In attempting to compare the various statistics of conventional and nuclear pressure vessels, two aspects where differences can occur must be given serious consideration :-

(a) With a conventional pressure vessel a thorough examination is carried out annually or biennially and any defects which are found, such as cracks etc., will be repaired, whereas major parts of a nuclear pressure vessel may be inaccessible for inspection after the reactor has gone critical, or may only be accessible for inspection at infrequent intervals and only after major dismantling work has been carried out. It is, therefore, necessary to consider serious defects which are found during inspection of conventional pressure vessels as well as the catastrophic failures of these vessels.

(b) In view of the potential hazards involved, all nuclear pressure vessels are subjected to extensive inspection during construction whereas the inspection carried out on conventional pressure vessels may vary from a service similar to that carried out on nuclear vessels, to very little inspection at all.

continued.....

With these two points in mind the scope of the survey was defined as follows :-

(a) Vessels should be of either welded or forged construction. Many riveted conventional pressure vessels and boilers are still in use and experience with these would not be relevant to nuclear pressure vessels.

(b) The vessels were constructed during manufacture to the current Class I requirements of B.S.1500, 1515, 3915, 1113, 2790, A.O.T.C. or other comparable standards at the time of construction. Table 1. illustrates the typical inspection stages for these codes from which it will be noted that the standards used are comparable with those required for nuclear vessels and in all cases include physical tests on plate material, procedure or production weld test plates and extensive non destructive testing of principle seams.

(c) A minimum wall thickness of 3/8" was specified as it was considered that this would be the minimum likely to be encountered in the nuclear pressure vessel fields.

(d) A minimum stipulated working pressure of 105 lb per square inch was specified as this would certainly eliminate any boilers built to standards lower than Class I and would also tend to eliminate any vessels which even though they were built to Class I standards were not, in fact, involved in onerous duties.

(e) Vessels older than 30 years were excluded as the present concept of a Class I standard with weld testing and non-destructive testing has only been in use in the United Kingdom for this period.

(f) Catastrophic failures were defined as those in which disruption of a vessel or of a component of a vessel necessitated major repairs or scrapping.

(g) Potentially dangerous failures were defined as defects requiring remedial action where the working conditions might result in a dangerous extension of a known defect. If a single reported occurrence involved several defects in separate components, these were all counted as failures.

(h) Failures of pipework built to comparable standards have been reported but this cannot be related to the total pipework involved.

Due to the way in which the Members of A.O.T.C. keep their records, it was initially necessary to rely on recollection of their staff to quote failures but since the reported recollections covering a 5 year period, comprehensive failure reports have been prepared at the time of the incident.

A standard form was used to report defects which gave details of the pressure vessel, its materials of construction, the working conditions to which it was subject, details of the defect, the method by which the defect was found and indications of the cause.

An estimated population of vessels within the scope of the survey was obtained from the Organization records.

continued.....

A detailed summary of the survey of failures for the five years up to 30th June, 1967, has been reported elsewhere (1) and Table II gives a numerical summary of these failures broken down by method of discovery and cause. The total population to which these defects relate, is about 100,300 vessel years.

It will be seen from Table II that the majority of failures (59%) were due to cracks and most of these were at branch connections and fillet welds. A more detailed summary of these failures is contained in Table III, from which it will be seen that Fatigue accounts for 40% of the cracks with the next most numerous class at 'not ascertained' at 30%.

In the more detailed study of the results carried out elsewhere (1) it is found that about 57% of all the failures reported were found by visual examination as compared with 9% found by Non-destructive or hydraulic testing.

A study of the age of the vessels which failed indicates that the more probable time for these incidents is in the early stages of service life which confirms the conclusion reported elsewhere (2).

Using the previously assigned definitions it can be concluded that the probability of a potentially dangerous defect occurring in a pressure vessel during service is 1.3×10^{-3} per vessel year and that of a catastrophic failure 0.7×10^{-4} per vessel year. It would appear that there is a factor of at least 10 between the probability of potential and catastrophic failure during service.

As the ultimate aim of the survey carried out is to obtain guidance for the service failure probability of nuclear reactor primary circuit envelopes, the reports of failure were studied with a view to eliminating defects which it was considered were irrelevant to the specific conditions experienced in nuclear pressure vessel envelopes. Nuclear primary circuits are unlikely to experience serious wastage, gross deformation or creep, because of design limitations. Mal-operation in reactors can be eliminated by rigid controls, however, undetected cracks may be present and pre-existing defects from manufacture caused through the employment of incorrect materials are not unknown in nuclear circuits. It was, therefore, considered that only defects due to cracks and pre-existing defects could be considered as relevant but the cracks were considered in more detail and approximately half of the cracks were eliminated as being ligament cracks, cracks in boiler furnaces, boiler furnace-to-end plate welds etc., etc..

Taking into account these further factors it is considered that the failure probability of defects in conventional vessels which are potentially dangerous and are relevant to nuclear primary circuits is approximately 6×10^{-4} per year and that the annual probability of catastrophic failures in conventional pressure vessels which are relevant to nuclear primary circuits is approximately 2×10^{-5} per year.

In this connection it is noted that Kellerman (3) quotes the probability of serious pressure vessel failures over a 7 year period as 9×10^{-3}. "Serious failures" are meant to describe a failure which would have caused a rupture of the pressure vessel during subsequent operation. The same author quotes the probability of pressure vessel failure over the same period as 2.1×10^{-4}

Continued...

In addition to the study of defects in pressure vessels during service, a study was made of vessels during construction and a record was kept of cases where defects were found during construction which required remedial action which were not detected or repaired during the normal inspection procedures (excluding the pressure test). These are cases where the Class I Pressure Vessel Inspection Service did not locate a potentially dangerous defect at the expected stage. Out of a total of 12,700 vessels involved, 10 incidents occurred. Two of the incidents are considered irrelevant to nuclear primary circuits as one involved a gas burner control failure and the other occurred during the purging of a vessel with liquid nitrogen. This gives a probability of 6.3×10^{-4} where significant defects have not been picked up during an inspection to Class I requirements.

In order to assess the relevance of this data to nuclear plant, an attempt has been made to survey the incidents occurring to reactor pressure circuit envelopes during normal operation. The information concerned has been based only on information published in the technical press and includes experimental reactors as well as power reactors. The study is limited to British and American reactors and covers 1,352 reactor years. It is agreed that in many cases the reactor primary circuit envelope is not subject to pressure but it is probable that in all cases the envelope has been built to a standard of construction comparable with Class I standards for conventional pressure plants. The actual incidents are reported in detail elsewhere (1) but it is noted that 17 defects, none of them catastrophic, have been reported which necessitated remedial action. This corresponds to an annual potentially dangerous failure probability figure of 1×10^{-2} which must be compared with a similar figure 6×10^{-4} from the results of the Class I pressure vessel survey so far. However, all figures relating to potentially dangerous defects are dependent on engineering judgement of the effect of any defect which is found and to whether remedial action is immediately necessary or not. The analytical study of the effect of different sizes and types of defects is as yet in its infancy. In addition to this, with reactor primary circuit envelopes not only is a determined effort made to locate any flaws which may appear during operation but also the detection of minute leakage may be facilitated by the presence of a slightly radioactive primary coolant. When a flaw is, in fact, located, it is more likely that a much more critical attitude will be taken to its presence than may be the case with the conventional plant.

Tables IV, V, VI and VII show the distribution of reports of failures during service, from the 18 months following the initial study of the A.O.T.C. survey, divided into 2 periods. The information relates to a vessel population of 7,800 vessel years for the last 6 months of 1967, and of 18,100 vessel years for 1968. In general the conclusions drawn from the earlier 5 year survey are confirmed and the deviation in 1968 of the number of failures found by N.D.T. and the 'Not ascertained' cause of cracks are due to a series of similar failures being reported in identical circumstances following a failure being found by visual inspection and an extensive programme of N.D.T. being started on all similar items.

If similar criteria to those used in the original survey are used, 3 failures can be eliminated from the last half of 1967 results, as not being relevant to Nuclear Primary circuit envelopes and 10 failures from 1968 results. None of the Catastrophic failure from 1968 can be eliminated.

Table VIII compares the results so far obtained from the survey for service failure rates.

continued....

Since June 1967, only one failure has come to light prior to commissioning. This relates to nozzle welds in chromium molybdenum vanadium steel boiler drum which was delivered to site but due to difficulties found elsewhere, an ultrasonic examination of the nozzles was carried out before hydraulic test and showed up serious cracking. During this period the ultrasonic examination of similar nozzles was commenced on a routine basis and but for this additional testing four other incidents which could have been classed as failure prior to commissioning would have been reported.

Arguments have been put forward that due to the inspection carried out during construction and the leakage which takes place before a catastrophic failure that it is impossible to envisage a sudden failure of this nature but one incident reported is of note in this connection. A 12½" diameter chromium molybdenum vanadium pipe to valve casting weld, failed completely leaving two open-ended pipes. The pipe was under steam pressure at a temperature of about 550°C. at the time of the failure and there was no evidence of leakage before the incident. Detailed examination of the failure indicated that the cracks initiating the failures were typical of stress relieving cracks and had been present since construction. These conclusions were confirmed when examination of a number of similar welds revealed serious similar cracking. The records showed that radiography, using the double-wall technique, had been carried out after stress relief and the welds passed as clear of defects. After the failure, the actual radiograph was re-examined and did not indicate the crack. This technique was in line with the Class I standards of inspection at the time of construction in 1964 and would have been similar to the inspection technique used in nuclear primary circuits.

A crack in the primary circuit of the Dounreay Fast Reactor (4) illustrates a similar case where a high degree of inspection did not indicate a defect which later caused a failure though fortunately only causing slight leakage in this case. The origin was finally found to be a crack in the weld of a 4" diameter pipe to a thermocouple block.

Detailed examination of the failed weld showed that there were some defects in the vicinity of the crack. First, the alignment of the pipe to the spigot of the block was badly out, there being a 0.049 in. misalignment between the two where the wall thickness was 0.080 in., giving a considerable step change in contour at this point. Also the weld tended to run off the line of the joint, and there was a lack of penetration giving rise to a stress raiser where the weld had a double start. The thermal stress was calculated to be within normal limits, but it is probably that without the stress failure would not have been caused by these defects alone. The radiograph of the weld concerned was found and re-examined.

Matthews has this to say about the case :-

"In accepting radiographs of these hand welds a certain amount of judgement usually had to be exercised, as by present day standards some of them are rather rough in appearance and uneven in contour, and therefore do not give perfectly clear radiographs. This is all right provided there is adequate thickness of the weld. The major contribution to the failure was the misalignment of the two sections of the pipe. The radiograph does not show that; the actual thickness of metal is there, but the sections are misaligned and the radiograph does not pick this up. On looking at this particular radiograph and comparing it with radiographs of a similar type, I think we would still pass it, taking into account that the weld was produced with the techniques available fourteen years ago.

continued...

The quality of welding has improved considerably since those times, and the radiographs which one would accept now are subject to more stringent limitations than those which were expected for the DFR."

CONCLUSION

At this stage it is considered that the information available on the failures of conventional and nuclear pressure vessels is limited. One of the major problems with this work which has not yet been fully resolved, is that with both conventional and, to a lesser extent with nuclear pressure vessels, defects are found by inspection before they have caused a catastrophic failure of the vessel itself and it is necessary to make an engineering decision based on a limited knowledge of the theories of failure to decide whether the defect concerned could have caused a catastrophic failure if the period between inspections had been greater.

In view of the extreme hazards involved, nuclear pressure primary circuit envelopes are usually constructed with a high degree of inspection during manufacture. However, from the limited work carried out so far, there is nothing to suggest that the incidence of potentially dangerous failures is likely to be significantly better than with relevant conventional pressure vessels.

REFERENCES.

(1) Phillips and Warwick, A Survey of Defects in Pressure Vessels built to High Standards of Construction and its relevance to Nuclear Primary Circuit Envelopes. A.H.S.B.(S) R.162. H.M.S.O. London.

(2) Phillips and Smith. An Analysis of Reported Boiler Explosions and its Implications for Safety of Pressure Vessels. A.H.S.B.(S) R.161. H.M.S.O. London.

(3) Kellerman. Present Views on Recurring Inspection of Reactor Pressure Vessels in the Federal Republic of Germany. I.A.E.A. Technical Reports Series No.81.

(4) Matthews and Henry, Location and Repair of a Leak in the Dounreay Fast Reactor Primary Circuit. B.N.E.S.Journal. Vol.8. No.3. July 1969.

INSPECTIONS	BS 2790 : 1956	BS 1113 : 1958	BS 1500 1958	BS 1515Pt. 1 : 1965	BS 3915 : 1965	ISO : R.831	ASME III : 1968
					(category A Vessels)		(category A Vessels)
Materials							
– visual, surfaces and edges	yes	yes	yes	yes	yes	yes	yes
– chemical analysis	"	"	"	"	"	"	"
– mechanical tests	"	"	"	yes – may specify elevated temperature tensiles also	yes – may specify elevated temperature tensiles also	verified hot proof properties of steel or may specify elevated temperature tensiles	"
– impact tests	–	–	low temperature service only	may specify	yes	–	yes
– U/S examination	–	–	–	–	"	–	"
Weld procedure and welder qualification tests	–	–	–	yes	yes	yes	yes
Examinations during fabrication							
– identification of materials	yes	yes	yes	yes	yes	yes	yes
– retention of test coupon plates	"	"	"	"	"	"	"
– parts formed to shape	"	"	"	yes	"	"	"
– edges prepared for welding	"	"	"	"	"	"	"
– alignment when assembled	"	"	"	"	"	"	"
– branches and openings prepared	"	"	"	"	"	"	"
– when seams back-chipped	"	"	"	"	"	"	"
– when welding completed	"	"	"	"	"	"	"
– after stress relief	"	"	"	"	"	"	"
Production weld tests (test plate attached to extension of welded seam)							
– test plate radiographed	–	–	–	(not required (unless specified	yes	(not required (unless specified	–
– mechanical tests	yes	yes	yes		"		–
Radiography							
– main longitudinal & circumferential seams	100%	100%	100%	100% (in certain cases may be 10%)	100% (U/S may be used after approval)	100%	100%
– other joints (includes all items of NDT)	–	"	–	(not required (unless specified	yes	–	yes
Stress relief	yes	yes	yes	yes – over 3/4" or 1.1/4" according to material	yes	yes – over 3/4" thick plate	yes
Pressure test (P=D) = pressure "new and cold"	1.5 P + 30 psi	1.5 P	1.5 Pn.c	1.3 Pn.c	1.25 Pn.c	1.5 P	1.25 Pn.c
Types of branch compensation allowed							
– compensating plates	yes	yes	yes	yes (special consideration if pressure/temp. fluctuations or low temps. involved)	no	yes	no
– integral	yes	yes	yes		yes (as full penetration weld attachment of nozzle)	yes	yes (as full penetration weld attachment of nozzle)
Fillet welds allowed	yes	yes	yes	yes	only as part of a penetration weld	yes	only as part of a penetration weld.

TABLE II

NUMERICAL SUMMARY OF FAILURES IN SERVICE

Defect Indication	Cracks	Corrosion	Mal-operation.	Pre-existing Defects from Manufacture	Creep	Total
V	70	1.U(1)1.F.	3.F(2)			75
L	36		1.U(2)		1.U	38
N.D.T.	9			1.U		10
H	1			1.U(4)		2
CAT	2		4.F(2)	1.U(3)		7
						132

NOTES

1. Erosion in a nuclear power station steam generating unit following the break up of a fabricated steel support structure. The debris in contact with a superheater tube eroded a hole.

2. Mal-operation causes were mainly shortage of water (4), oil contamination (2).

3. 10 in. diameter, 3/8 in. thick steam pipework burst for about 10 ft. longitudinally, due to laminations. After the first failure further laminated pipes were found by ultrasonic methods.

4. Superheater header suffered serious cracking and was replaced in a different material.

CLASSIFICATION AND ABBREVIATIONS.

U. = Unfired component

F. = Fired component

CAT = Failure found by a catastrophic occurrence

L = Failure found by leakage

H = Failure found by hydraulic testing

V = Failure found by visual examination

N.D.T.= Failure found by non-destructive testing methods.

TABLE III

NUMERICAL SUMMARY OF CRACKS OCCURRING DURING SERVICE

POSITION	CRACK INDICATION	CAUSE					
		Fatigue	Corrosion	Pre-existing from Manufacture	Not Ascertained	Miscellaneous	Total
(i) Boiler furnace or furnace to end plate weld. Shell boiler back tube plate cracking.	V	8.F		1.F	1.F	1.F(1)	11
	L	6.F				1.F(1)	7
(ii) Cracks in welded branches and fillet welds	V	8.U(3)	12.U(3)	3.U(4)	6.U(5)		29
	L	5.U(2)					5
	N.D.T.		2.U.	1.U	1.U		4
	CAT			1.U(4)			1
(iii) Cracks along the length of a weld	V	9.U(6)	2.U				11
	L	4.U(6)					4
	N.D.T.			2.U	3.U		5
(iv) Cracks in parent plate material	V		1.U				1
	L			1.U			1
	CAT	1.U(7)					1
	H	1.F					1
(v) Tube to tube plate ligament cracking	V.	1.U	4.F		1.F.6.U		12
	L	1.F			12.U		15
(vi) Cracks radiating from openings	V		1.U.2.F.				3
(vii) Cracks in pipework (all unfired)	V	1.U(8)			2.U		3
	L	2.U		1.U	3.U		6
							118

Notes:

1. The two miscellaneous failures were due to the failure of the refractory lining at oil burning equipment on furnaces.
2. Two failures on similar vessels rotated on trunions. Two failures of pipework with defective supports.
3. The 20 fatigue and corrosion assisted fatigue failures are related to steam receivers at power stations in the region of branches.
4. Two cases of header inspection caps, one was blown out under working conditions; the boilers concerned were similar.
5. Four of these failures relate to cracks in fillet welds of baffles or fixings. One of these involves BS 1501-620B material, where a crack penetrated a 3/4 in. thick header in 6 months.
6. Nine failures of jackets of vessels subject to a steam-cooling water cycle.
7. Failure of very high pressure pipe originating from internal surface defects.
8. Crack in a corrugation extending 80% round the circumference but not detected by leakage.

TABLE IV

NUMERICAL SUMMARY OF FAILURE IN SERVICE - LAST 6 MONTHS OF 1967

Defect Indication.	Cracks	Corrosion	Mal-operation	Pre-existing defects from Manufacture.	Creep	Total
V	5			1 F (1)		6
L	6					6
N.D.T.						
H						
CAF						
						12

NOTE: 1. Laminated plate in shell boiler furnace - part of plate burnt away.

TABLE V

NUMERICAL SUMMARY OF CRACKS OCCURRING DURING SERVICE - LAST 6 MONTHS OF 1967

Position	Crack Indication	CAUSE					Total
		Fatigue	Corrosion	Pre-existing from manufacture	Not ascertained	Miscellaneous	
i) Boiler furnace or furnace to end plate weld. Shelf boiler back tube plate cracking	L	1 F					1 F
	V	1 F					1 F
ii) Cracks in welded branches and fillet welds.	L	2 U					2 U
	V	1 F					1 F
iii) Cracks along the length of a weld.	L				3 U		3 U
	V				1 U		1 U
iv) Cracks in parent plate material	V	2 U					2 U
							11

For classification and abbreviations see TABLE II

TABLE VI

NUMERICAL SUMMARY OF CRACKS OCCURRING DURING SERVICE - 1968

Position	Crack Indication	Fatigue	Corrosion	Pre-existing defects from manufacture	Not Ascertained	Miscellaneous	Total
(i) Boiler furnace or furnace to end plate weld. Shell boiler back tube plate cracking.	L V CAT	3 F 1 F(1)				1 F	3 F 1 F 1 F
(ii) Cracks in welded branches and fillet welds.	V L N.D.T.	2 U			1 U(2) 12 U(2)		1 U 2 U 12 U
(iii) Cracks along the length of a weld.	V				1 U		1 U
(iv) Cracks in parent material							-
(v) Tube to tube plate ligament cracking							-
(vi) Cracks radiating from openings							-
(vii) Cracks in pipework (all unfired)	CAT	2 U(4)		1 U(3)			3 U
							24

NOTES:
1. Failure of a shell boiler furnace seam originating from undercut at toe of fillet weld. There is record of previous mal-operation of boiler.
2. 13 cases relate to cracks in the nozzle welds of boiler drums. The exact cause is still under investigation. Other instances have been found which have not yet necessitated repairs.
3. Referred to in text.
4. Both seams on boiler feed pipework - one major circumferential failure from root of triform junction reinforcement.

TABLE VII

NUMERICAL SUMMARY OF FAILURE IN SERVICE - 1968

Defect Indication.	Cracks	Corrosion	Mal-operation	Pre-existing defects from manufacture	Creep	Total
V	3		2 F (1)	1 F(2)		6
L	5					5
N.D.T.	12					12(3)
H	-					-
CAT	4		2 F(1)			6
						29

NOTES: 1. Four cases of shell boiler furnace deformations or failures due to shortage of water.
2. Part of furnace tube burnt away due to area of serious laminations in plate.
3. All twelve cases relate to similar incidents where cracking was found in nozzle attachments. They were found as the result of an extensive programme of testing of similar items.

TABLE VIII

COMPARISON OF FAILURE RATES FOUND DURING SERVICE

Class of Failure	5 years : 1962-1967	Last 6 months 1967	1968
All potential failures	1.3×10^{-3}	1.5×10^{-3}	1.6×10^{-3}
All catastrophic failures	7×10^{-4}	None reported	3.3×10^{-4}
Potential failures considered relevant to nuclear circuits.	6×10^{-4}	12×10^{-4}	10.5×10^{-4}
Catastrophic failures considered relevant to nuclear circuits.	2×10^{-5}(1)	None reported	1.1×10^{-4}(2)

NOTES: 1. The catastrophic failures include one case of pipework (50% of total)
2. These catastrophic failures all relate to pipework (2 failures)

For classification and abbreviations see TABLE II

Commission des Communautés Européennes
EURATOM
C.C.R.- ISPRA

Engineering Department
Technology

Meeting of specialists on the reliability of mechanical components and systems for nuclear reactor safety

24th-26th September 1969

ASPECTS OF DESIGN RELIABILITY OF PRESSURE TUBES FOR HEAVY WATER MODERATED REACTORS

M.MOFTAGHANI and J.PUTZEYS

JP/kdv
ENR/C-IE/714/69

Summary

The core of a pressure tube heavy-water moderated reactor is made up of a light vessel throughout which are passing parallel channels, each consisting of a cold calandria tube and a hot pressure tube.
The design of the pressure tube must be based on the strength of the material, on neutron absorption and on economical considerations.
The allowable probability of an accident (a channel burst or a pressure tube burst) and the corresponding economical damage must be connected mutually.
For a heavy water moderated and organic liquid cooled reactor, it is proposed to use SAP (Sintered Aluminium Powder) to fabricate the pressure tubes.
A test program was performed to study the consequences of a pressure tube burst, i.e. strains introduced in the neighbouring channels, in the vessel and in the safety systems.
The long term mechanical resistance of SAP is determined by its creep behaviour. A statistical analysis of experimental creep rupture test results allows to determine the thickness of the pressure tubes for a certain rupture probability under normal operating conditions.
Using the results of both studies a reliability concept can be introduced to determine design criteria for the pressure tubes.

1. Introduction

A high-power heavy-water moderated reactor with pressure tubes is characterised by a bundle of between 500 and 1000 parallel channels (vertical or horizontal). Each channel consists of a hot pressure tube containing the fuel elements which are cooled by gas, water or organic liquids and a cold calandria tube which isolates the pressure tube from the moderator.

In contrast to the relatively sturdy construction of the channels, whose pressure tubes must be able to withstand the pressure of the coolant, the vessel itself is large and particularly light. This is because under normal operating conditions it only needs to withstand a low pressure. Under accident conditions, however (a pressure tube burst, which would lead to the bursting of the calandria tube) the vessel and vessel-internals are strained by pressure waves which, in certain cases, can cause considerable damage [1].

Arguing in statistical-economical terms the probability of a channel (pressure tube + calandria tube)-burst, which has serious consequences, i.e. causes considerable economic damage, must be kept particularly low. On the other hand, one can admit a much higher probability for the burst of a pressure tube only, for which the consequences are much less severe, because they are confined within the calandria tube.

There is, however, another factor, i.e. the neutron economy, that limits the indefinite increase of the pressure tube thickness, especially for natural uranium reactors. Thus, one can not reduce indefinitely the rupture probability of the pressure tube.

The thickness of the pressure tube is therefore defined by the optimalization of the reactor as a whole, and finally it is the overall economy balance which is decisive. This paper does not deal with the whole problem of optimalization, but only discusses some design and economical aspects which may contribute to the solution of the problem.

2. The consequences of a pressure tube rupture

There are various cases to be considered, depending upon whether the coolant employed is gas, water or organic liquid. Where gas or water is employed as coolant, the high pressure permits only the pressure tube (because of the neutron absorption) to be designed to withstand the coolant pressure. Therefore, if the pressure tube should burst, the calandria tube (normally a Zirconium alloy tube with a thickness of less than 1 mm), which has not been dimensioned to withstand high pressure, will consequently also burst. This must be considered to be a severe accident; the coolant mingles with the moderator, and fuel element fragments may be hurled against the neighbouring channels and damage them. It has nevertheless been proved by the experiments performed for the CIRENE reactor (Holtbecker and Leoni, unpublished) that the bursting of one channel does not lead to a chain of bursts in the other channels. The consequences of this accident therefore consist of:

a) the need to replace the entire channel, i.e. pressure tube and calandria tube,
b) the recovery of parts of the fuel elements
c) possibly, some of the neighbouring channels which have been damaged but not destroyed need to be replaced,
d) the exchange of polluted heavy water in the case where the coolant employed is light water.

In order to carry out such an operation, the reactor would have to be shut down for several months.

An estimation of the relative cost should take into account both repair costs and the greater costs for the supply of the energy from other sources.

On the basis of these elements one can estimate the cost of the accident to about 7-8% of the capital, i.e. about 100-150 dollars per kWe installed [2]. The probability of such an accident should therefore be kept very low. How low these probability must be will be determined, as told beforehand, by the optimalization of the reactor as a whole.

Referring to what other authors [3] admit for the chance of failure for pressure vessels, it is estimated that the probability of 1 in 10^4 during the design life for the accident described before can be considered conservative, thus the pressure tubes in Zircaloy, that normally are used in the water or gas cooled reactors, must satisfy these specifications.

When an organic liquid cooled reactor is considered, the situation is different because of the low pressure of the coolant. In fact in this type of reactor the calandria tube, with the same thickness as that foreseen for a water or gas cooled reactor, can withstand the pressure of the coolant circuit (pressure less than 30 Ata), in case the pressure tube ruptures.
It is therefore possible to combine the rupture probability of the pressure tube and of the calandria tube.
Taking into consideration also the bellows and the other components of the primary circuit, one can, by a good design, easily limit the rupture probability to a value less than 1 in 100.
Thus in order to have for the whole channel, pressure tube and calandria tube, the same conditions as for a channel of a water or gas cooled reactor (rupture probability 1 in 10^4) the thickness of the pressure tube must be such that the rupture probability will be 1 in 100.
The following chapter will show what thickness for a hot pressure tube of SAP has to be used to satisfy the above specifications.

3. Creep rupture of a hot pressure tube

3.1. Creep test program

It has been established that the best criterion for calculating the allowable stress in SAP is its creep-rupture behaviour.
The permissible stress is then defined as the stress causing rupture after a certain time with a certain probability. A creep test program was therefore initiated on tube sections at two temperatures, 420°C and 300°C respectively.
The test sections consist of a 850 mm long SAP tube, 3 mm thick and with an internal diameter of 92 mm, closed at both ends by stainless steel plugs allowing a leak tight closure to be realised. An internal SAP filler connects the two plugs, thereby both eliminating axial stresses on the tube and reducing the volume of the pressurized gas.
The creep tests on tube sections were done in monoaxial stress conditions (eliminating axial stresses) thus allowing to compare these results with those of a series of tests performed on tensile specimens [4].

3.2. Statistical Analysis

To obtain reliable results from creep-rupture tests it is necessary to analyse the experimental data by statistical methods [5]. One has to establish a relation between stress and time-to-rupture and to determine what destribution law is verified for the experimental data.

The empirical creep law proposed in the literature relates the stress σ and the time-to-rupture t in the form :

$$\log t = A + B\sigma,$$

This relation is verified for ductile materials, and will be assumed valid also for SAP, because actually there are too few experimental results available to show whether another empirical law would fit the creep data better.

A Kolmogorov test showed that the normal distribution law did fit best the observed results, confidence level 0,91 [6]. Now the confidence intervals for the creep-rupture data will be determined.

A first confidence interval must be calculated for the domain in which experimental results are available. In that domain the magnitude of the confidence intervals depends not only on the scatter of the data but also on their number. The fewer data are available the wider the confidence interval, for a constant confidence level, will be.

A second confidence interval is calculated for the extrapolated domain, in which a confidence level for the regression line has to be considered. The greater the ratio of the extrapolated interval to the experimental interval is, the wider the confidence interval will be.

The size effect, i.e. the increase of rupture probability with increase in size, is a factor that may be critical for the design with brittle materials, and has been calculated for SAP that behaves in a brittle way in creep conditions [5].

3.3. Results

Two series of tests were done at 420°C and 300°C respectively. The allowable stress is calculated as the stress causing rupture after 2.10^5 hrs (30 year life time) with a probability of 1%.

The numerical results for the allowable stresses for the SAP pressure tubes (full length i.e. 5 m) is given in table 3.3.1.

table 3.3.1

	300°C	420°C
regression line	log t = 17,4 - 1,99 σ	log t = 12,6 - 2,09 σ
standard deviation	0,587	0,796
allowable stress : 1% probability of failure	3,15 kg/mm^2	1,5 kg/mm^2

Because creep tests are very time consuming experiments, results are only obtained at two temperatures. A linear interpolation is felt to be a pessimistic approximation, and could be used to estimate an allowable stress for the SAP pressure tubes at an intermediate temperature.

The values of the allowable stresses can be converted in terms of pressure tube thickness if the operating conditions are defined. An organic cooled reactor can have for instance a primary cooling circuit operating with inlet conditions 20 atm and 300°C and outlet conditions 8 atm and 400°C. The thickness of the pressure tubes in SAP must than be about 4 mm; not taking into consideration other limiting factors as e.g. wear.

4. Conclusions

The reliability approach, as applied to the safety of the vessel-internals of a reactor, allows the thickness of the pressure tube to be determined by rules which are independent of the normal calculation codes. The problem is thus transferred from the traditional basis to a more realistic approach, inasmuch as it is now based on economic concepts.

This concept may be generalised for the design of any structure of a reactor (e.g. pressure tubes in Zircaloy, pressure vessel, vessel internals) and not only if these structures are subjected to creep but also under conditions of static stresses, of fatigue etc...

The example discussed (SAP pressure tube) is only an example demonstrating the method. The choice of the pressure tube should be made, in this particular case, in comparison with other solutions [7] on the basis of the optimalization of the reactor as a whole.

Acknowledgements

The authors wish to thank Mr. H.Holtbecker for information on safety experiments performed on pressurized water tubes, Mr. C.Rinaldini for technical-economic information, Mr. C.Albertini who did the metrology and the non-destructive tests of the tube sections, and Messrs. P.Gritzmann and D.Del Torchio who performed the experimental work.

REFERENCES

[1] "Full scale Experiment on the Consequence of the rupture of a Pressure tube in ESSOR reactor vessel" by H.Holtbecker, M.Montagnani and G.Vorneletti - EUR 4101 f.e.

[2] "Kernbrennstoff Bedarf und Kosten verschiedener reaktorentypen in Deutschland" by H.Büsse, G.Gubta

[3] "A new approach to reactor safety Evaluation and Siting" by F.R.Farmer, Safeguards Division, Authority Health & Safety Branch U.K.A.E.A., Risley

[4] "Non-destructive and destructive testing of reactor pressure tubes in SAP" by C.Albertini, M.Montagnani and P.Weltovreden - EUR 3929 e.

[5] "Statistical interpretation of creep data for the evaluation of design criteria for reactor pressure tubes" by M.Montagnani and J. Putseys - ASME conference on "Pressure vessels technology"- Delft, Sept. 1969.

[6] Private information by D.Basile

[7] "Nuclear reactor channel with Zirconium alloy pressure tube at optimum operating temperature" by P.Parfaletti Casali and M.Montagnani - Nuclear Engineering and Design (6 - 1967).

LA FIABILITE DES PROPULSEURS A REACTION DIRECTE

par

A. MIHAIL * BUREAU VERITAS

Le transport aérien a connu depuis la dernière guerre et notamment durant cette dernière décade, un développement prodigieux. La mise en ligne des avions de transport à réaction n'a fait que confirmer cette tendance.

Le progrès technique s'est traduit par un accroissement notable du confort, de la capacité, de la vitesse (celle-ci est passée de 140 km/h en 1925 à 320 km/h en 1940 pour atteindre plus de 900 km/h aujourd'hui).

Toutefois, il faut le reconnaître, l'avion inspire encore à bien des usagers et surtout à la masse de ceux qui n'ont pas été touchés par ce nouveau moyen de transport, un sentiment d'inquiétude en raison du caractère de gravité que représente l'accident aérien, aussi rare soit-il. (A noter toutefois que d'après l'IATA, le coefficient de sécurité, fonction du taux d'accident mortel par km/passager parcouru, a plus que doublé en dix ans).

En effet, il est bien connu que le grand ennemi de l'avion c'est le risque et sa conséquence directe : l'accident.

Celui-ci, outre la perte d'un matériel coûteux (un Boeing B. 707 ou un Douglas DC. 8 valent de trente à cinquante millions de francs), peut entraîner des pertes de vies humaines et susciter une réaction immédiate chez le passager qui peut conduire, dans certains cas, jusqu'à une désaffection pure et simple pour un matériel donné en particulier (par exemple, la première version

...

* Ingénieur du Génie Maritime
Ingénieur Militaire de l'Air (CR)
Ingénieur Principal au Bureau Veritas
Chargé de cours à l'Ecole Nationale de l'Aviation Civile
Maître de Conférence à l'Ecole Supérieure Nationale de l'Aéronautique
Président de la Commission de Fiabilité de l'Association Française des Ingénieurs et Techniciens de l'Aéronautique et de l'Espace

de l'avion de transport Lockheed Electra) et pour le transport aérien en général.

Les retards enregistrés au départ sur des horaires préétablis, bien que ne mettant pas toujours en cause directement la sécurité, ont eux aussi une influence indiscutable sur les usagers en laissant planer une vague atmosphère d'insécurité, surtout lorsque la cause (cas assez fréquents) n'est pas indiquée clairement.

Tout ceci conduit à rechercher dans le transport aérien un haut degré de sécurité.

Les facteurs qui conditionnent la sécurité du transport aérien peuvent être classés en trois catégories :

a) - Facteurs extérieurs au matériel lui-même (navigation aérienne, environnement etc...)

b) - Facteurs d'utilisation du matériel (conditions d'exploitation, équipages etc...)

c) - Sûreté de bon fonctionnement du matériel.

Par ailleurs, les acquéreurs d'un avion de transport (qui sont aussi souvent les utilisateurs) ne considèrent plus le matériel comme un bien consommable, mais désirent avoir la garantie de la possibilité de son exploitation régulière pendant un minimum de 30 à 40.000 heures de vol (à raison d'une moyenne de 10 heures par jour), soit durant 10 à 12 ans (le matériel étant ensuite rebuté par déclassé techniquement).

Lorsque l'on regarde l'entrée d'air des groupes générateurs de puissance d'un B. 707 ou d'un DC.8, la marque de l'un des plus grands constructeurs de moteurs d'avions, apparaît entourée de sa devise "dependable engines", autrement dit "moteurs sur lesquels on peut compter".

.../...

Les intéressés font là plus qu'une profession de foi, ils mettent en évidence une condition essentielle pour un propulseur aéronautique, à savoir sa sûreté de fonctionnement.

En effet, le groupe générateur de puissance a pour mission principale d'arracher à la pesanteur l'aéronef et sa charge (constituée en général de passagers) et de permettre de véhiculer cet ensemble dans des délais de plus en plus réduits sur des parcours de plus en plus importants; il ne peut donc être question d'appliquer à cette partie essentielle de l'aéronef, la boutade du marchand de parachutes qui dit : " Il n'y a pas de problèmes, tous les parachutes qui ne s'ouvrent pas, je les remplace gratuitement ".

1.- DEFINITION DE LA FIABILITE

C'est justement la nécessité de l'étude scientifique approfondie des conditions requises par une sécurité de bon fonctionnement qui a donné lieu à cette nouvelle discipline que les anglo-saxons ont baptisée du nom de "RELIABILITY" et qui a été traduit en France par le néologisme "FIABILITE" ou "sûreté de fonctionnement".

Il n'a, malheureusement, pas été établi à l'heure actuelle une terminologie internationale concernant cette nouvelle discipline. Aussi, les définitions en présence sont-elles multiples.

Nous avons retenu, pour notre part, celle proposée par la RADIO ELECTRONES TELEVISION MANUFACTURERS ASSOCIATION à savoir :

" La fiabilité est la probabilité pour qu'un
" équipement, appareillage ou composant assure
" sans défaillance les opérations pour lesquelles
" il a été prévu, durant une période de temps et
" dans des conditions de fonctionnement définies.

La fiabilité apparaît donc comme une probabilité fonction du temps. Aussi est-il coutumier de l'exprimer en probabilité de bon fonctionnement en % par période d'emploi (celle-ci étant fonction des caractéristiques d'utilisation et pouvant être exprimée en cycles, nombre de tours, temps), soit pour plus de commodité en % de probabilité de défaut par période d'emploi.

2.- IMPORTANCE DE LA FIABILITE

La figure 1 (qui ne se réfère ni à un matériel déterminé ni à un utilisateur donné mais représente une moyenne) permet d'apprécier l'importance des anomalies (et donc de la fiabilité) sur les différents éléments constitutifs d'un aéronef (en fonction de la phase où ces anomalies sont survenues).

Un propulseur à réaction directe, plus connu sous le vocable de réacteur ou "jet" est un ensemble composé de plusieurs milliers de pièces importantes (3100 dans le cas du Pratt et Whitney JT 4, 3800 dans le cas du Rolls Royce Avon).

La fiabilité a également une influence sur l'aspect économique de la réalisation et de l'exploitation du matériel aérospatial. Ainsi, il a été calculé que la mauvaise tenue en service du matériel coûte à la ROYAL AIR FORCE environ 3 milliards de francs annuellement (auxquels il faut ajouter 45 millions par suite d'accidents matériels). La ROYAL AIR FORCE est conduite à remplacer annuellement 50 % de ses 50.000 microswitches et de ses 10.000 pompes auxiliaires à carburant par exemple. Aux U.S.A., le maintien en état de fonctionnement du matériel électronique de la Marine représente durant la première année de livraison, le double du prix d'achat. C'est-à-dire qu'au bout de 10 ans on a dépensé 20 fois le prix d'achat pour l'entretien. Enfin, en France, la part des crédits consacrés à l'achat de pièces de rechange avoisinait 25 % du total des crédits alloués à l'électronique par le Ministère des Armées.

.../...

L'étude de la fiabilité permettra d'acquérir des élémente sur : l'amélioration de la sûreté de fonctionnement, le choix d'un matériel le mieux adapté aux besoins, les conditions d'entretien, l'organisation rationnelle des stocks.

3.- FIABILITE DES COMPOSANTS ELEMENTAIRES ET DES ENSEMBLES

Que ce soit pour les composants élémentaires ou pour les ensembles complexes, les définitions applicables en ce qui concerne la fiabilité seront sensiblement les mêmes.

Il est toutefois bien évident que si la panne d'un composant élémentaire met pratiquement fin à son existence, tel ne sera pas le cas de l'ensemble complexe où la défaillance d'un des composants peut n'entraîner que son changement et donc la remise en service de l'ensemble (à condition, bien entendu, que l'ensemble soit réparable ou récupérable). Ceci suppose l'application de mesures de maintenance préventives afin de réduire au maximum le risque de panne.

Quoi qu'il en soit, il convient de distinguer, pour un composant ou un ensemble, les conditions de fonctionnement propres (limites, critères de défaillance, critères de fonctionnement, contraintes) et les conditions dues à l'exploitation (dont certaines sont connues et définies - tel l'entretien -, alors que d'autres - telles les conditions réelles de fonctionnement dans des contraintes d'environnement facteur humain - ne le sont ou ne peuvent l'être qu'avec une assez grande approximation).

Dans le cas des conditions de fonctionnement propres (conditions plus rapprochées de celles du laboratoire), la fiabilité du composant ou de l'ensemble est plus communément appelée "fiabilité intrinsèque", alors que dans le cas des conditions dues à l'exploitation, la fiabilité est plus connue sous l'appellation de "fiabilité d'exploitation". Le produit de ces deux fiabilités constitue la fiabilité dite "opérationnelle" qui correspond, en fait, aux résultats effectivement atteints en exploitation réelle.

.../...

La fiabilité des ensembles se calcule plutôt qu'elle ne se mesure en raison de la taille et du prix des unités et des difficultés à réaliser des essais complets.

Un propulseur à réaction directe est un ensemble de plus en plus complexe où se trouvent rassemblés simultanément des phénomènes thermo-aérodynamiques, chimiques, physiques, électriques, etc... (qui eux-mêmes ne sont pas moins complexes). Il apparaît donc qu'il est difficile d'affirmer qu'il puisse être obtenu une probabilité absolue de parfait fonctionnement (ou que la probabilité de panne soit nulle).

L'examen des figures 2, 3 et 4 montre la variation de la fiabilité des pièces constitutives.

La figure 2 montre la variation de la fiabilité d'un système lorsque le nombre de ses éléments varie, chaque élément ayant une fiabilité propre de 99 %. Si l'ensemble est composé de 10 éléments sa fiabilité est encore élevée (90 %); si l'ensemble est composé de 100 éléments, la fiabilité du système diminue à 36 %. Enfin, elle ne sera plus que de 3 % pour 400 éléments. Ce dernier chiffre est cité car il représente, ainsi que nous le verrons par la suite, le nombre approximatif de "pièces sérialisées" dans un réacteur.

La figure 3 indique justement la variation de la fiabilité d'un ensemble composé de 400 éléments, en fonction de la fiabilité de chaque élément. Si chaque élément a une fiabilité propre de 99,5 %, la fiabilité de l'ensemble n'est que de 14 % alors qu'elle sera de 70 % si la fiabilité de chaque élément est de 99,9 %.

La figure 4 donne le réseau de courbes permettant de déduire en fonction du nombre d'éléments constituants et de la fiabilité propre de chacun, la fiabilité d'un ensemble complexe. Il convient de noter que si l'on considère les 3 100 pièces principales d'un JT 4, par exemple pour arriver à une fiabilité de cet ensemble de 70 %, la fiabilité de chaque élément devra être supérieure à 99,985 %.

.../...

L'examen de ces différentes figures permet de formuler deux remarques :

a) La fiabilité d'un ensemble est, d'après la théorie même de la probabilité composée, le résultat de la valeur fiable de chaque élément constitutif. Ces éléments doivent être considérés comme des éléments indépendants qui concourrent à un objectif commun, par exemple l'obtention dans des conditions précises de certaines performances (qui seront assurées par la combinaison d'un certain nombre de fonctions élémentaires). Ceci suppose que la prédétermination des conditions de fonctionnement dans le dispositif étudié est bien acquise et qu'il n'y a pas de réaction "parasite" des éléments, les uns sur les autres.

b) Il apparaît que la fiabilité d'un système n'est jamais que celle de son élément critique le plus faible mais la fiabilité de cet élément peut être changée, soit en y modifiant les conditions de son utilisation, soit en lui apportant des modifications technologiques (exemple : au début de l'utilisation des réacteurs Avon sur la Caravelle, certaines anomalies ont été enregistrées sur le roulement central; une modification technologique consistant à diminuer sa charge par augmentation du chemin de roulement, a permis d'améliorer sa fiabilité propre).

4.- ASPECT QUALITATIF DE LA FIABILITE

La sélection systématique, la mise au point et la vérification du bon fonctionnement d'un propulseur avant sa mise en service, nécessitent des mois (voire des années). Ceci provient du fait que la fiabilité des composants élémentaires et des ensembles devra être une oeuvre de création continue à tous points de vue et à tous les stades. Aussi, elle devra être "pensée" dès le stade de l'avant-projet (prévision de la fiabilité) jusqu'à mise en exploitation effective (maintien et amélioration de la fiabilité). En effet, une fois le matériel conçu et réalisé, on ne peut plus faire grand chose pour améliorer la fiabilité.

.../...

En règle générale, les facteurs fondamentaux qui déterminent la probabilité de survie d'un élément ou ensemble sont les aléas du processus de fabrication et les caractéristiques aléatoires des efforts que l'élément doit supporter en fonctionnement (contraintes dues à l'environnement ou aux conditions de fonctionnement).

La conception, l'expérimentation et la fabrication devront tenir compte de ces exigences et ceci non pas uniquement pour l'élément prototype mais surtout pour la série (qui en fait seule intéresse l'utilisateur). Il conviendra à cet effet, de prendre toutes dispositions (notamment sur le plan du contrôle de la qualité) afin que la fiabilité des séries successives ne se trouve pas abaissée pour quelque raison que ce soit.

Autrement dit, dès le début, la facilité d'entretien obtenue par l'application des principes de démontabilité, accessibilité et interchangeabilité, devra retenir l'attention. Il est nécessaire par exemple que les principaux composants ou divers ensembles puissent être démontés comme des ensembles indépendants et sans que l'opération influe de façon notable sur les autres sous-ensembles; ceci aussi bien en cas d'inspection que de réparation.

4.1.- La fiabilité au stade de l'avant-projet et de l'étude

Au stade avant-projet et étude, il conviendra de définir un certain nombre de paramètres ayant une influence directe sur la fiabilité. Les plus importants de ces paramètres apparaissent comme étant :

- Les performances demandées à l'ensemble et notamment les limites à l'intérieur desquelles, l'ensemble sera considéré comme "bon" (à titre d'exemple, dans le cas d'un aéronef, une vitesse de croisière inférieure de 10 km/h à celle annoncée, peut représenter pour un exploitant, une perte de l'ordre de 50 000 fr par appareil et par an).

.../...

- Les conditions prévues d'obtention de ces performances : conditions d'emploi, conditions d'environnement, etc.. (par exemple, l'Avon équipant la Caravelle, effectue un cycle de décollage - donc de conditions limites - environ toutes les 90 minutes, alors que le JT 4, équipant le Boeing, accomplit ce cycle dans les conditions actuelles d'exploitation prévues, toutes les 3 heures 1/2 environ) (fig 5)

- La durée d'utilisation envisagée.

Il convient de remarquer que les solutions proposées ou retenues aux différents problèmes aérodynamiques, thermiques, métallurgiques, permettent déjà implicitement de se faire une idée du degré de fiabilité d'une pièce ou d'un ensemble (par exemple, le choix d'un système de refroidissement des aubes de turbine constitue une amélioration certaine du degré de fiabilité, non seulement des aubes elles-mêmes mais également de l'ensemble. Il convient de noter que dans le bilan général, la solution du refroidissement des aubes est assez séduisante, car peu coûteuse. En effet, pour le refroidissement des premier et deuxième étages des aubes de guidage de turbine et du premier étage des aubes mobiles, du Rolls Royce Spey, la consommation spécifique de ce moteur ne se trouve majorée que de 0,5 %).

L'étude des conditions d'emploi peut, par ailleurs également permettre de détecter, dans certains cas, les composantes les moins fiables. Par exemple, si l'on sait que le réacteur est destiné à être utilisé en zone sablonneuse, le compresseur pouvant subir un phénomène d'érosion, on peut l'éviter, en partie, soit :

- en utilisant un matériau adéquat,
- en utilisant des grilles sur l'entrée d'air (avec toutefois les inconvénients que cela peut entraîner).

Il en va de même d'une analyse préalable des pompes. L'étude, par exemple, de la direction du jet à la sortie de l'inverseur ou du déviateur, permet de se rendre compte s'il n'y a pas de risques d'ingestion de corps étrangers.

Il est bien évident

.../...

Nous constatons donc que dès ce stade, il est pratiquement indispensable de faire l'option entre un matériel destiné à l'usage civil ou militaire. Il est, en effet, coutumier de dire que les militaires recherchent la performance, alors que pour les civils, la durée d'utilisation ou si vous préférez l'endurance, en raison de son influence sur l'aspect économique du problème, est un facteur primordial. Il apparait donc vain de vouloir "adapter", après coup, un propulseur à une tâche différente de celle prévue, à moins bien entendu, d'accepter d'y mettre le prix (cela a été le cas des Rolls Royce Avon de la série militaire 200, devenue 500 pour la version civile, des Pratt J 57, devenus JT 3 et J 75 transformés en JT 4, encore que cette dernière transformation n'a pu être achevée complétement, notamment en ce qui concerne l'accessibilité et la démontabilité; en effet, le carter compresseur est d'une seule pièce, ce qui entraîne un empilage des disques et entretoises, avec obligation d'enlever tous les disques qui précèdent celui ayant une avarie) (1976)

Compte tenu de ce qui précède, certains peuvent penser qu'il peut y avoir difficultés de cohabitation entre la notion de performance et la fiabilité. C'est perdre de vue le paramètre "temps" entrant dans la définition de la fiabilité (exemple : le satellite et son lanceur : si les deux ensembles doivent avoir des fiabilités élevées pour assurer des performances particulières - performances, il est vrai de nature différente : du domaine de la propulsion pour le lanceur, du domaine de l'électronique et des transmissions pour le satellite - le temps pendant lequel ces performances sont demandées, s'exprime en secondes ou minutes pour le lanceur alors que pour le satellite, il s'exprime en mois, voire en années).

Enfin, pour le matériel civil, il est également essentiel de considérer à ce stade, l'endurance comme une performance qu'il conviendra de rechercher et d'obtenir au même titre qu'une basse consommation spécifique, par exemple.

.../...

4.2.- La fiabilité au stade des études et de la mise au point

Il convient de distinguer, parmi les principaux éléments constitutifs d'un propulseur, trois groupes d'éléments :

Dans un premier groupe :

- Les éléments structuraux dont la défaillance peut affecter directement la sécurité (cas des ensembles tournants, etc...). Autrefois, les pièces de cette catégorie avaient des coefficients de sécurité très importants (on n'utilisait certaines pièces qu'au dixième de la charge de rupture). Aujourd'hui, la prise en considération du principe du "self containment", d'une part, et l'application du système de construction dit du "fail safe", d'autre part, permettent une diminution du poids des pièces et donc une amélioration des performances.

Pour les pièces vitales, les risques de défaillances acceptables généralement admis sont de l'ordre de 10^{-8} par heure de fonctionnement. Ces pièces sont donc surabondantes ou ont une redondance élevée pour employer le langage des électroniciens.

A ce sujet, il est nécessaire d'ouvrir une parenthèse :

Il est bien évident qu'un pareil chiffre mène à la négation de l'interprétation statistique (car c'est la fin de la loi des grands nombres) et conduit, en fait, à suivre les pièces une à une, en établissant un facteur limite de sécurité. C'est là, l'origine des pièces dites "sérialisées" qui sont repérées et suivies individuellement du point de vue durée de fonctionnement, modification, etc... par les constructeurs ou réparateurs à l'aide de véritables fichiers.

En pratique, cette probabilité de panne de 10^{-8} fait apparaître comme nécessaire d'affecter un temps limite de fonctionnement des pièces envisagées.

Ce temps peut être déterminé à l'aide d'essais accélérés faits au banc ou en laboratoire. Il est bien évident

.../...

que ces essais sont coûteux, tant pour ce qui est de l'appareillage, que du temps nécessaire, ou de l'outillage à mettre en oeuvre, et ce, d'autant plus que la fiabilité recherchée est plus grande. Ces essais ont surtout pour objet d'étudier les lois d'accélération des phénomènes en fonction des contraintes. Les disques de turbine et compresseur, par example sont soumis, si on néglige les phénomènes de corrosion, à des sollicitations à haute fréquence d'origine aérodynamique à leur périphérie, mais la fatigue, surtout pour les disques de turbine est due également à des sollicitations à basse fréquence d'origine thermique. Les essais de simulation concernant ce type de sollicitations peuvent être faits sur moteur au banc ou à l'aide de machines spéciales en laboratoire. Pour certains des réacteurs en service, un nombre de 6 000 à 10 000 cycles environ, a été estimé, après essais, comme admissible. Ceci peut conduire, compte tenu de la durée du parcours moyen pour un utilisateur donné, à des durées de vie moyennes différentes pour une même pièce (de l'ordre de 12 000 à 16 000 heures de fonctionnement pour les disques de compresseur ou turbine).

Il est permis également de se poser la question concernant la corrélation entre les résultats des essais accélérés et les conditions d'exploitation réelles.

Dans certains cas, cette corrélation pourra être établie à l'aide d'un ou plusieurs paramètres définis dans les spécifications d'essais.

En fait, les essais accélérés permettent :

a) de faire connaître à l'utilisateur si la qualité livrée par le constructeur a évolué; autrement dit, ils donnent un renseignement très rapide sur un problème particulier,

b) d'apprécier la valeur d'un résultat par comparaison (dans le cas de l'application d'une modification par exemple).

Il est toutefois évident que les essais accélérés ne peuvent être que des repères et doivent être confirmés par des résultats obtenus en exploitation. En effet, dans l'étude

.../...

de l'influence de la température, par exemple, les lois de vieillissement accéléré sont assez malaisées à définir et donc à vérifier.

Voici pour le premier groupe de pièces. (fig 7)

Dans un deuxième groupe, il convient de distinguer les éléments pouvant causer des dommages secondaires important (roulements principaux, aubes mobiles, réducteurs).

Outre les essais particuliers auxquels ils ont donné lieu au stade de la mise au point, c'est surtout le taux de panne élevé relevé en service qui constitue le princip critère de fiabilité. Pour certains roulements, par exemple, Rolls-Royce admet comme limite 0,01 incidents par 1 000 heures de fonctionnement, soit une fiabilité de 0,99 par 1 000 heures A ce sujet, il est à noter que d'après une étude faite par TALLIAN, 10 % du total des anomalies des roulements se produisent dans la tranche des premiers 4 % du temps total de fonctionnement admis pour ces pièces.

L'ensemble des pièces de ce deuxième groupe constitue une autre catégorie de pièces dites "sérialisées" (ou nécessitant un suivi particulier).

Enfin, dans un troisième groupe de pièces sont classés tous autres éléments susceptibles d'avoir une limite de vie (carter compresseur, entrée d'air, chambre, etc...).

En résumé, à ce stade, l'étude du spectre des contraintes devra permettre, compte tenu de l'expérience déjà acquise par ailleurs, des conditions d'emploi et des processus entraînant les défaillances ou l'usure, de déterminer celles des contraintes qui sont les plus sensibles et donc qui influent directement sur la fiabilité. Il sera alors possible de prévoir des composants ou ensembles ayant des coefficients de sécurité surabondants (ou redondants) [redacted] ou de "dévaluer" les composants en les soumettant à un fonctionnement sous contraintes réduites.

.../...

C'est également à ce stade qu'il convient d'apporte toute l'attention à la facilité d'entretien en tenant compte des exigences de démontabilité (démontage d'une pièce sans détérioration de la pièce voisine), interchangeabilité (possibilité de substitution d'une pièce à une pièce semblable) accessibilité (possibilité d'accès facile aux différents organes et pièces).

L'adoption pour les réalisations pratiques des systèmes dits "des blocs fonctionnels" assurant des fonctions bien précises et susceptibles d'être démontés, entretenus et remontés séparément, sont des éléments importants dans l'amélioration de la fiabilité.

4.3.- La fiabilité au stade de la fabrication de série

A ce stade, en vue de garantir une bonne fiabilité, il convient :

- de faire appel, pour la mise en oeuvre, à des procédés de fabrication éprouvés (matière, main-d'oeuvre, outillage, etc...).
- d'assurer un contrôle poussé de la qualité (à noter à cet effet que la fiabilité ajoute une dimension nouvelle au service contrôle de qualité en lui donnant la possibilité de prolonger ses investigations dans le temps).

4.4.- La fiabilité au stade des essais

A ce stade qui constitue un des éléments les plus importants de la fiabilité car il est aussi celui de la sélect: finale, il convient de remarquer qu'il ne s'agit pas uniquement de savoir quel est le matériel bon ou mauvais au départ ainsi qu'éventuellement, la dispersion de ses caractéristiques, mais il importe de dire combien de temps le matériel pourra conserve ses caractéristiques initiales et les dispersions de celles-ci en fonction du temps.

En règle générale, il convient d'admettre que plus la fiabilité recherchée sera élevée, plus les essais devront être nombreux, longs et coûteux. En effet, on ne connaît pas d

.../...

lois rigoureuses qui régissent les variations de la fiabilité suivant les régimes de fonctionnement et donc le niveau des différentes contraintes.

Les essais d'endurance (qui doivent être considérés comme des essais complémentaires des essais de vérification de performances et d'ambiance) s'avèrent par ailleurs indispensables pour déterminer la politique d'entretien préventif à suivre (pour les matériels à longue durée de vie) ou pour garantir que les phénomènes d'usure ou "de dérive" des différents composants n'affectent pas le fonctionnement de l'ensemble durant l'exécution de sa mission.

Ceci peut être recherché également à l'aide d'essais dans des conditions d'ambiance (rayonnement, en température, vibrations, etc...).

En raison des conditions exigées dans certains cas (vérification de risques de défaillance de l'ordre de 10^{-8}, etc...), des moyens à mettre en oeuvre, du coût et du temps nécessaire, les essais réels s'avèrent quelquefois difficiles, voire inconcevables. Aussi fait-on appel de plus en plus aux tests séquentiels et, en particulier, aux essais accélérés.

Ceux-ci peuvent être envisagés au banc ou en laboratoire. Ils ont surtout pour objet d'étudier les lois d'accélération des phénomènes en fonction des contraintes et permettent d'apprécier le niveau de fiabilité par comparaison à une limite préétablie.

4.5.- La fiabilité au stade de l'utilisation

A ce stade, la fiabilité sera garantie par une série de contrôles indicatifs précis et rigoureux de certains paramètres et de l'état des pièces.

.../...

L'ensemble de ces opérations est plus connu sous le nom d'entretien (autrement dit opérations ayant pour but de maintenir les performances d'un équipement au niveau spécifié à l'aide d'une série de mesures prédéterminées).

Ce stade représente, en aéronautique, un pourcentage assez élevé des dépenses d'ensemble (voir figure 8 - frais horaires d'utilisation d'un quadriréacteur).

Actuellement, il existe deux types de contrôle indicatif :

- Le premier type est représenté par les visites périodiques, destinées surtout à "prévoir" et non "à guérir" appelées communément "inspections". Le but principal de ces visites est de permettre de détecter toute anomalie et d'apprécier la possibilité de survie d'une pièce ou d'un ensemble, compte tenu des critères préétablis. Ces inspections peuvent être permanentes ou occasionnelles et des changements de pièces peuvent y être programmés systématiquement.

Il convient de mentionner ici, la place de plus en plus importante prise par les enregistreurs de paramètres techniques et les détecteurs de pannes. Ces dispositifs ne font, en fait, que maintenir un état d'inspection continu.

- Le second type de contrôle indicatif est représenté par les révisions destinées à permettre de porter sur chaque pièce, après démontage complet de l'ensemble, un jugement sur son état, en vue d'apprécier la possibilité de remise en service pour une période de temps déterminée (ceci après simple contrôle ou reconditionnement, voire modification de la pièce).

Dans les deux cas, il s'agit de prévenir les pannes causées par la variation lente d'un ou plusieurs paramètres (dont l'usure mécanique ou la "dérive" des performances constituent des aspects particuliers).

Toutefois (la ou les) lois de dégradation sont en premier lieu fonction de l'usage que l'on demande à la pièce ou à l'ensemble et des mesures prises en vue de son entretien.

.../...

Ceci implique, sur le plan pratique, l'assurance que les travaux programmés sont rigoureusement suivis par les intéressés, aussi bien au stade de l'entretien (inspections), que de l'utilisation (limites et procédures opérationnelles).

Ce qui précède ne veut pas dire que le rôle du facteur humain se trouve diminué ou limité, bien au contraire, mais qu'il faut également tenir compte d'un certain pourcentage d'anomalies dues à la défaillance humaine, pourcentage qui doit intervenir directement dans l'appréciation du niveau de fiabilité.

Enfin, à l'aide de la théorie des processus stochastiques et en utilisant la simulation sur calculateur électronique, l'utilisateur pourra, par exemple, définir les conditions d'un entretien préventif efficace, les prévisions concernant les matériels à réparer, les pièces de rechange à réapprovisionner, les stocks complémentaires à constituer.

4.6.- La fiabilité au stade de l'après-vente

Une place primordiale doit être accordée à l'analyse des pannes produites en exploitation qui constitue pour l'amélioration de la tenue du matériel, un important élément de guidage.

C'est là un point auquel, malheureusement, les producteurs ne semblent pas apporter l'attention qu'il mérite. Et pourtant, l'intérêt que cela représente, aussi bien pour l'amélioration de la tenue en service d'un matériel donné, que pour la renommée d'un fabricant, n'est plus à démontrer. Qu'il suffise de se rappeler que certains matériels ont été éliminés du marché faute d'un suivi efficace. Le Service Après-Vente ne devrait pas se limiter à traiter les problèmes économiques mais proposer également aux utilisateurs des solutions propres à satisfaire les aspects techniques de leurs problèmes.

L'impression prévaut actuellement que, dans certains secteurs, les constructeurs n'ont qu'une vague idée du comportement de leurs productions et des frais d'entretien occasionnés par le maintien du matériel en service. Il

.../...

s mblent porter au contraire toute leur attention (ce qui p urrait être considéré comme normal) sur l'importance des v ntes des pièces de rechange.

5.- ASPECT ECONOMIQUE DE LA FIABILITE

Le problème de la fiabilité, outre son aspect t chnique qui vient d'être développé, a également un aspect é onomique d'importance primordiale pour les utilisateurs.

En effet, en vue d'assurer une exploitation s re et rentable, les utilisateurs devront, en premier lieu, p océder à un bilan économique global.

Dans ce contexte, la fiabilité n'est qu'un des é éments d'appréciation du problème économique d'ensemble q i devra tenir compte :

- du prix d'achat (sur lequel la plupart du temps, l'utilisateur n'a qu'une possibilité d'action relativement réduite),
- du prix d'entretien (où l'influence exercée par l'utilisateur peut être très importante),
- et du prix des pièces de rechange.

Autrement dit, pour l'utilisateur qui ne pourra, b en entendu, méconnaître les aspects techniques du problème, l fiabilité, c'est l'art d'obtenir une exploitation correcte d son matériel, au moindre prix. Mais cela ne veut pas dire q e la meilleure fiabilité représente toujours l'optimum é onomique et le rôle déterminant des responsables des compagnies s riennes consiste justement à trouver le meilleur compromis e tre le coût de "détection" et le coût "d'élimination de l anomalie".

Un exemple : il a été dit précédemment qu'au s ade d'utilisation, la fiabilité sera assurée par une série d contrôles indicatifs. Cependant, il convient d e ne pas p rdre de vue que si, à l'origine, c'est le constructeur qui p évoit ces contrôles, c'est en fait, l'utilisateur qui les e écute (directement ou indirectement) et qui en subit les c nséquences économiques.

.../...

Autrement dit, en règle générale, une inspection nécessite :

- un certain temps d'immobilisation (l'heure d'immobilisation d'un Boeing coûte 4 000 $),
- des frais de main-d'oeuvre (la révision d'un réacteur nécessite environ 1 500 heures),
- certaines dépenses inhérentes (le banc d'essai, par exemple, dont les frais peuvent représenter 3 à 4 % du prix total d'une révision),
- le prix des pièces de rechange (ce prix peut atteindre dans certains cas environ 45 % du prix total de la révision).

Dans ces conditions et en respectant les impératifs de sécurité, il peut y avoir un choix économique à faire entre les possibilités offertes par le remplacement à des périodes déterminées d'un plus grand nombre de pièces pour réduire l'importance de certaines inspections et inversement.

La figure 9 montre la relation existant entre le prix de revient et la fiabilité.

6.- ASPECT PSYCHOLOGIQUE DE LA FIABILITE

Ainsi que précisé au début de cette communication, la fiabilité doit être "pensée" dès le commencement d'une étude et doit être considérée comme une création continue.

Aussi, à l'intérieur d'une entreprise (de production ou d'exploitation), il sera bon de prévoir une organisation fonctionnelle qui puisse constituer un système d'information et de contrôle intéressant (du point de vue de la fiabilité), l'ensemble des activités.

Cette organisation devra :

- définir les aspects quantitatifs de la fiabilité.
- diffuser les données quant aux aspects qualitatifs de la fiabilité. (Il conviendra de ne pas confondre contrôle de qualité et fiabilité qui sont en fait complémentaires),

.../...

- définir les caractéristiques des éléments et ensembles (ainsi que les tolérances) à partir des spécifications finales relatives au produit complet,
- fermer les boucles du contrôle afin que tout incident signalé fasse l'objet d'une analyse et de mesures correctrices,
- renseigner l'utilisateur (ou le fabricant) pour lui permettre d'apporter, en ce qui le concerne, les mesures correctives,

  A cet effet, il convient de noter qu'il serait souhaitable que le degré de fiabilité soit spécifié à l'utilisateur, au même titre que les autres caractéristiques.
- faire les recommandations et indiquer le choix pour la réalisation d'éléments les mieux adaptés du point de vue fiabilité.

Il est toutefois bien évident que cette organisation sera fonction de l'importance et de la nature de l'entreprise.

7.- CONCLUSIONS

Quelles sont les perspectives d'avenir et notamment pour l'avion supersonique ?

Les progrès techniques dont bénéficieront les réacteurs auront une répercussion certaine sur l'amélioration de leur fiabilité. Toutefois, cette évolution est prévisible et circonscrite. A titre d'exemple, on espère peu d'améliorations sur le rendement adiabatique de la turbine qui est actuellement de l'ordre de 93 % ou du rendement polytropique du compresseur (de l'ordre de 90 %). Il en va de même pour les matériaux où les améliorations escomptées apparaissent comme intéressantes, mais non révolutionnaires.

.../...

Par contre, il est certain qu'une amélioration notable de la fiabilité peut être obtenue par l'exploitation scientifique, grâce aux ordinateurs électroniques, des analyses préalables de pannes : que ce soit les pannes simples, doubles, triples ou les pannes dormantes. Il y a là un champ d'activité notable offrant des perspectives particulièrement prometteuses, aussi bien du point de vue de la sécurité que de la fiabilité et ceci d'autant que le point faible du réacteur actuellement ne semble plus être constitué par le moteur lui-même, mais plutôt par ses accessoires et les circuits.

La notion de potentiel, telle qu'elle est conçue aujourd'hui, est également appelée à évoluer. En effet, il convient de remarquer que le secteur entretien dont nous avons montré l'importance et l'influence sur la fiabilité, est loin d'avoir suivi, aussi bien dans la conception que dans la réalisation, le progrès technique matérialisé par la mise en ligne des avions à réaction ; les faibles réductions des frais d'entretien rapportées à l'heure de vol obtenues avec ces avions, ne sont en effet réalisées que grâce aux améliorations propres des caractéristiques du matériel (vitesse, matériaux etc...).

Actuellement, les exploitants sont en train de prendre conscience du fait que les travaux d'entretien ne doivent plus être exécutés à des périodicitée fixes, mais seulement s'ils s'avèrent indispensables. Cette façon d'envisager le problème est susceptible de représenter non seulement une amélioration de la sécurité, mais également une augmentation de rentabilité du matériel par diminution des durées d'immobilisation et augmentation des durées de vie.

Toutefois, ce qui précède, n'est au demeurant valable que si, en appliquant une méthode d'entretien nouvelle, l'on parvient à surveiller l'état de fonction-

.../...

nement du matériel, d'une façon permanente. Cette surveillance doit permettre de déceler les premiers indices de défaillance et de localiser les pannes. Les phénomènes à développement lent (par exemple : baisse de puissance graduelle) et les défaillances subites devront être détectées et il sera nécessaire d'obtenir une indication précise sur l'endroit, l'étendue de la panne et sur les causes possibles. A titre d'exemple, des détecteurs de vibration ont permis, en 22 mois d'exploitation, de détecter 34 % du total des anomalies survenues sur les réacteurs Conway.

Par ailleurs, il convient que ces renseignements soient utilisables à des fins de comparaison dans des délais réduits. Autrement dit que l'exploitation de paramètres enregistrés durant un vol de plusieurs heures puisse être faite pendant les quelques dizaines de minutes nécessaires à une escale.

Une anomalie détectée suffisamment à temps est incomparablement moindre que si elle avait pu produire tous ses effets. Sur le Tyne, par exemple, l'utilisation de bouchons magnétiques sur le circuit d'huile, a permis de tripler les cas de détection d'avaries de roulements. Or, lorsque l'on sait que les gros réacteurs tournent à 8000 - 10 000 tr/mn alors que les petits atteignent plus de 40 000 tr/mn, on mesure l'étendue des anomalies pouvant être causées par un incident de roulement.

En appliquant cette nouvelle méthode, la durée de vie ne se trouvera plus ainsi être limitée à une périodicité fixe, mais sera en fait, fonction des résultats de détection.

A titre d'exemple, il convient de signaler que la Military Air Transport Service (M.A.T.S.), qui est le

.../...

plus important transporteur mondial et qui constitue en même temps un excellent banc d'essai, étudie ce problème à grande échelle, aussi bien pour les propulseurs que pour les cellules. Ces études sont faites à l'aide d'appareils enregistreurs d'un poids et d'un encombrement réduits (grâce aux progrès de la microminiaturisation). Certains de ces appareils pouvant enregistrer simultanément plus de 1500 paramètres différents.

Il y aura évidemment, le moment venu, un problème de fiabilité propre aux différents systèmes de détections, mais cela constitue un autre aspect de la question.

Tel est, Messieurs, le problème dont je m'étais proposé de vous entretenir. Comme vous avez pu le constater, le sujet étant très vaste, non seulement, je ne l'ai pas épuisé, mais sur certains points, faute de temps, je regrette de n'avoir pu essayer de vous éclairer davantage.

J'espère toutefois, vous avoir donné un aperçu des questions qui sont en réalité, si intimement liées à celle de la sécurité.

Je serais très heureux, si pour certains d'entre vous, ces quelques réflexions ont pu être de quelque utilité.

Je vous remercie de votre attention.

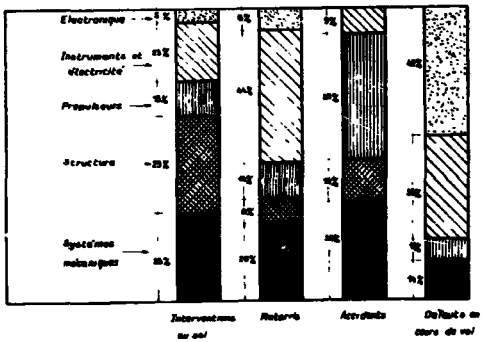

Electronique
Instruments et électricité
Propulseurs
Structure
Systèmes mécaniques
Interventions au sol
Retards
Accidents
Défauts en cours de vol

Fig. 1.

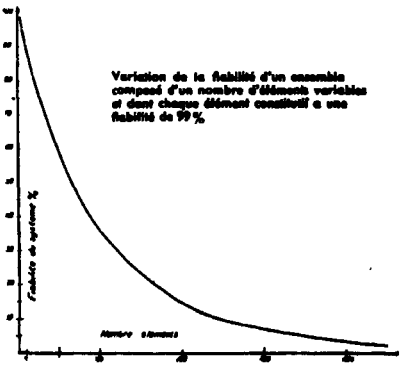

Variation de la fiabilité d'un ensemble composé d'un nombre d'éléments variables et dont chaque élément constitutif a une fiabilité de 99 %
Fiabilité de système %
Nombre éléments

Fig. 2.

Ensemble composé de 400 éléments
Variation de la fiabilité de l'ensemble
en fonction de la variation de la fiabilité
de chaque élément composant.

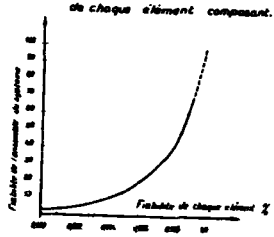


Fig. 3.

Fiabilité des composants et des parties

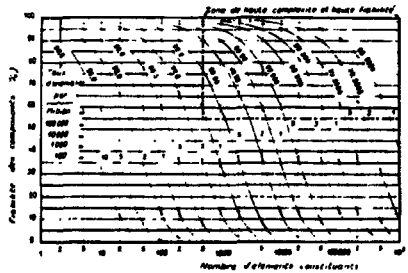


Fig. 4.

Relations entre le coût des pièces de rechange et le nombre de décollages.

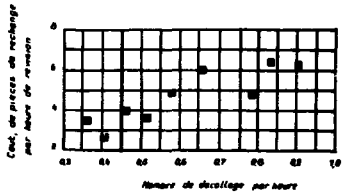


Fig 5

	Poussée lbs	N° Cert. de classification	Débit d'air lbs/sec	Température de fonct. °K	Rapport de compression	Rapport de pression de fonct.	Puissance kilowatts	SFC (kg/kg/h)	Nbre de réacteurs Plans
Avec Lighting Compresseurs 16 étages Turbines : 3 étages	12 700	6000	170	1200	8,00	8,7	400	600000	20
Avec 727 Caravelle Compresseurs 16 étages Turbines : 3 étages	11 700	6000	170	1210	9,10	9 à 9,5	3000	1000000	10

Fig. 6.

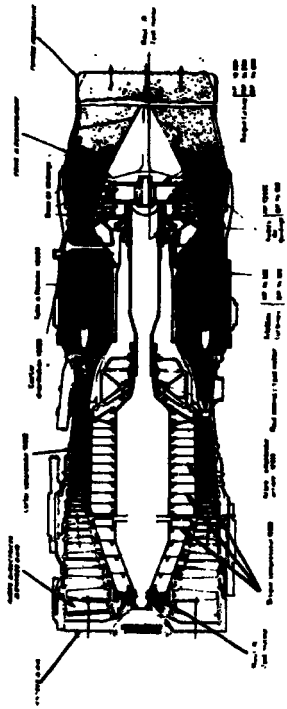
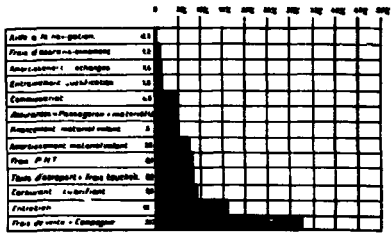


Fig. 7



Répartition des frais pour une heure de vol

Fig. 8

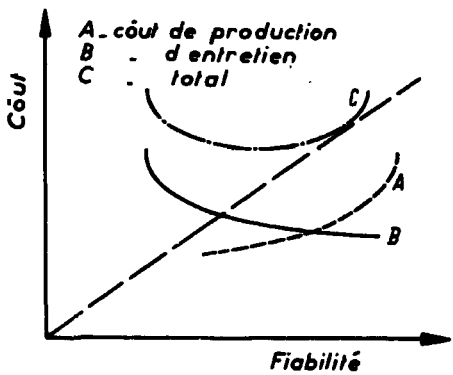


Figure 9

DIRECTION DES MATÉRIELS EN EXPLOITATION

COLLECTE ET UTILISATION DES INFORMATIONS CONCERNANT LE COMPORTEMENT DES MATERIELS

Présentation par Madame G. ARNAUD
Ingénieur à la Direction des Matériels en Exploitation
au ENEA/CREST meeting - RISÖ (Danemark)
24 - 26 Septembre 1969

D. M. E. 69.07.08

Complément à la conférence

COLLECTE ET UTILISATION DES INFORMATIONS CONCERNANT LE COMPORTEMENT DES MATERIELS

(Mme ARNAUD - SNECMA)

La brochure qui vous a été remise, a été écrite en vue de présenter un exemple précis de réseau d'information.

Vous pouvez y trouver :

- d'une part des généralités sur les objectifs qui ont conduit à le créer et les résultats qui peuvent être obtenus
- d'autre part des détails sur l'étendue du réseau, les secteurs étudiés, les paramètres relevés, les codes utilisés, etc...

Au cours des minutes qui me sont accordées, je voudrais, non pas m'attarder sur ces détails, mais au contraire ajouter quelques remarques qui se rapportent à l'état d'esprit qui doit imprégner chaque maillon du réseau, état d'esprit qui, tout autant que les techniques de l'informatique, contribue à la réussite du système.

C'est ainsi que la qualité de l'information recueillie est primordiale. La collecte doit donc se faire avec une certaine rigueur et cela contrarie bien sûr de vieilles habitudes ou oblige certains à préciser leur pensée.

En outre le traitement de ces informations sur ordinateur peut mettre facilement en évidence des erreurs ou anomalies non seulement à l'échelon du technicien qui a fourni l'information, mais encore à l'échelon des structures des services.

Malgré tout il faut que cette collecte soit considérée comme un outil efficace pour la connaissance des matériels et non comme un maillon d'un réseau de surveillance.

De même il ne faut pas que le Client à qui il est demandé des informations précises sur l'utilisation, l'entretien et les pannes de ces matériels, considère ces demandes comme une ingérence dans son exploitation.

Ensuite il faut sans cesse affirmer, bien que cela paraisse une évidence qu'un fichier même s'il porte le nom pompeux de banque de données ne peut produire que ce qui a été prévu de produire lors de sa conception.

Il peut cependant être extensible, quant au type de matériel à suivre.

Enfin il faut préciser que le système décrit, s'il fait largement appel aux moyens des ordinateurs et des mathématiques statistiques, n'exclut pas la présence d'une équipe d'ingénieurs et de techniciens. Cette équipe doit, en effet, ajouter le bon sens et la réflexion indispensable pour augmenter l'efficacité des résultats et transmettre ceux-ci de façon sélective et adaptés aux besoins de chacun.

De nombreuses publications ont déjà largement traité des avantages qui peuvent être retirés du suivi de matériels, surtout lorsque ceux-ci sont des machines à hautes performances dont la fiabilité doit sans cesse être améliorée et pour lesquels un coût d'exploitation minimum est recherché à travers une définition adéquate de la maintenance et du volume des rechanges à mettre en place.

Dans cette lutte difficile où la sécurité et l'économie doivent trouver leur compte, il devient nécessaire de conjuguer les efforts des constructeurs, des utilisateurs et également des organismes officiels de normalisation ou de contrôle.

Cette brochure n'a donc pas la prétention de démontrer à nouveau la nécessité de poursuivre de tels objectifs dont chacun est d'ailleurs convaincu du bien fondé, mais de faire part de quelques particularités d'un système fonctionnant actuellement à la SNECMA pour des moteurs militaires et, lorsque cela est possible, des idées directrices du projet de suivi des moteurs Olympus qui équiperont l'avion Concorde.

Historique :

Depuis dix ans, la SNECMA se préoccupe d'organiser les renseignements relatifs à l'utilisation de ses matériels.

1ère phase.

La première étape a été la mise en forme mécanographique des informations provenant des Utilisateurs, communiquées par ses représentants détachés sur les Bases.

Cela a permis de connaître, non seulement les défaillances observées avec leurs circonstances, l'âge des matériels en cause, mais également le parc des matériels contrôlés et maintenus en service. Dès lors, il était possible d'établir :

- des statistiques à but technique (pour orienter par exemple des études de modification)

.../...

- des courbes de fiabilité (selon la méthode actuarielle) pour définir des familles de pièces selon les phénomènes d'usure et de défaillance, pour situer une limite de potentiel

- des courbes de prévision de déposes et leur application à un plan d'utilisation donné.

Motifs d'une nouvelle orientation.

Bientôt, il s'est avéré que les renseignements ainsi traités ne reflétaient plus qu'une fraction trop petite de la vie des matériels.

a) En effet, ceux-ci avaient vieilli, avaient été réparés plusieurs fois, mais une partie seulement avait été remplacée ou rénovée. Il importait donc de connaître lors du nouvel incident si la partie détériorée était ou non d'origine et quels en étaient alors les âges depuis 1ère mise en service, et depuis dernière réparation.

b) Les standards avaient également évolué de nombreuses fois et il n'était plus possible de distinguer aisément (sans étudier un nouveau réseau d'information) des populations homogènes.

c) La périodicité des contrôles devenant progressivement de plus en plus grande (actuellement dans le rapport de 1 à 4 depuis la mise en service), il se faisait que pour des pièces dont les détériorations ne se manifestent pas immédiatement par un mauvais fonctionnement, il n'était plus que rarement constaté des anomalies en utilisation alors que des détériorations nombreuses étaient sans doute constatées en usine au démontage.

En conséquence, il devenait difficile, voire même impossible, de pouvoir répondre aux questions de plus en plus nombreuses posées par les différentes directions.

.../...

Définition d'un nouveau système :

Recensement des objectifs.

Pour l'ensemble des moteurs civils et militaires diverses catégories d'objectifs ont été définies ainsi que les travaux standards correspondants. (Voir annexe 1).

Etude d'un système "Fichier Central".

Pour répondre aux principaux objectifs retenus en liaison avec les directions intéressées de la Société, il a été créé un groupe de travail groupant des représentants de ces Directions.

Au cours des réunions il a été examiné qu'elles étaient :

a) - les informations existantes à transformer automatiquement

b) - les informations existantes à réécrire sous forme adaptée au traitement sur ordinateur

c) - les informations existantes ou non, pouvant être relevées lorsque le système serait mis en application

d) - les informations existantes qui ne pourraient pas être introduites "en rattrapage".

Il a été adopté comme principe que :

- chaque secteur ne transmettrait que les informations dont il serait "producteur"

- les paramètres ou caractéristiques ne feraient l'objet d'inscriptions multiples que pour des motifs impératifs d'enchainement d'informations et de traitement.

Etendue du réseau d'information.

Dans la vie d'un matériel, trois grandes phases sont à considérer.

Construction.

- **Fabrication** : fiche d'identification du matériel, N° de coulée ou de forge, standard...

- **Montage** : fiche donnant la composition d'un ensemble, ex : arbres et pignons d'un renvoi de commande.

.../...

- Essais : fiche précisant les conditions et temps d'essai.

- Documents de livraison.

(Toutefois, parmi ces documents, ceux relatifs aux pièces détachées appartiennent à un autre fichier géré par le Département Rechanges).

Les informations sont inscrites sur des supports envoyés directement en perforation.

Utilisation.

Pour tout événement relatif à un matériel désigné pour être suivi, il est établi un rapport,

. soit sur un support quelconque, transformé par le bureau central des statistiques,

. soit sur un support pré-codé,

. soit sur un support directement perforable.

On considère qu'un événement se produit lorsqu'il y a :

- opération de maintenance ou d'inspection (programmée ou non)
- application de modification
- variation même momentanée de performances, de valeur de paramètres
- mouvement de pièce (d'un moteur à un autre, mise provisoire en volant...).

Réparation.

Pour tout matériel entrant en réparation, des fiches sont établies systématiquement au niveau de l'ensemble suivi ; en outre, les composants détériorés font l'objet de fiches complémentaires.

Principales catégories de paramètres.

Pour une pièce faisant l'objet d'un suivi, il est relevé notamment, pour chaque événement la concernant :

- son identification :
  - désignation
  - n° de plan
  - n° de série individuel
  - n° du support sur lequel elle est montée

.../...

- son état au moment de l'événement :
  - neuf, réparé, RG
  - nombre d'unités de vieillissement
  - nombre d'heures total depuis fabrication
  - position

- les circonstances au moment de l'événement :
  - en vol, au sol, au point fixe,
  - contrôle sur avion, au banc...

- les manifestations ou effets ressentis

- les constatations faites :
  - nature des défauts
  - emplacement des défauts
  - importance des défauts
  - narration complémentaire avec mots clés

- les décisions prises ou envisagées (mise en réparation, expertise
  (rebut
  (maintien en service
  (application de modification
  (application de consigne
  (application de solution de réparation
  (etc...

Codes. Pour les moteurs civils, les codes utilisés sont le plus souvent des codes ATA complétés par des codes Société.

Réalisation :

Organigramme
annexe 2.

- Collecte
- Traitement
- Exploitation

Supports de collecte de l'information
annexe 3.

Quelques exemples de supports pour le recueil de l'information :

3-A - Recueil des informations "Utilisation" sur Olympus pré-série.

3-B - Recueil des informations "Réparation" pour ATAR 9 K.

3-C - Recueil des informations pour l'évolution du standard des pièces.

Code
annexe 4.

Un exemple de code particulier "ATAR" pour le relevé des défauts.

Cette annexe regroupe pour le redresseur de turbine :

a) Les catégories de défauts définies par le Contrôle et mentionnées dans la documentation officielle (utilisateurs et réparateurs).

b) Les localisations d'autres défauts pouvant être décelés.

Il est donné, en outre, un schéma de localisation pour l'anneau de turbine 1er étage afin de faire remarquer que des zones situées sur un même axe ont des codes rattachés entre eux.

Exemple : 3 W (redresseur de turbine)

1 W (anneau de turbine)

ceci est utile pour l'établissement de statistiques, corrélation de défauts par rapport à un fonctionnement donné, influence de la configuration géométrique en amont de la pièce défectueuse.

Traitement.

La description des traitements n'est pas l'objet de cette réunion. Il est seulement signalé que ceux-ci sont réalisés sur IBM 360/40.

.../...

Suivi de la composition et du vieillissement d'un parc :

Il a été mentionné précédemment les circonstances pour lesquelles était établi un rapport ou document.

Ces circonstances sont le plus souvent, soit une constatation d'avarie, soit un contrôle de fonctionnement ou d'aspect. Or, il se peut que ces circonstances se produisent peu fréquemment et il faut donc compléter le système précédent par une mise à jour de la composition et du vieillissement du parc d'un type de matériel donné.

En ce qui concerne les matériels civils, il a été imaginé le système automatique suivant.

Etant donné que :

a) La composition d'un moteur est connue à sa livraison,

b) Lorsqu'il y a changement de pièce un rapport est établi,

c) La pièce montée en remplacement est connue soit
parce qu'elle a appartenu à un autre moteur,
parce qu'elle a été livrée au titre de pièce détachée,
il est notamment connu son temps de fonctionnement (nul ou non) au moment de son dernier montage,

ce parc des pièces peut être connu en tant qu'identité d'individus.

Il faut, en outre, en connaître les âges à un moment donné.

Pour un matériel aéronautique, la fréquence de mise à jour idéale serait "le vol".

Après chacun d'eux (la composition du moteur n'ayant pu varier entre le début et la fin)

. ou bien il y a un rapport d'incident

. ou bien l'ensemble des pièces a vieilli en fonction de l'activité moteur.

Il suffit alors d'introduire en ordinateur les caractéristiques du vol écoulé et d'affecter les mêmes Δ u aux pièces constitutives du moteur au départ du vol.

Il semble un peu utopique d'espérer des informations aussi fréquentes. Moyennant quelques complications de programme, il sera possible d'obtenir des résultats mensuels, mais alors il faudra tenir compte des modifications intermédiaires des compositions de moteurs.

Unités de vieillissement :

Il apparaît de plus en plus que si l'évaluation du vieillissement en heures est commode, elle masque par contre un certain nombre de phénomènes importants quant à la connaissance de la fiabilité du matériel.

En aéronautique notamment, où les séries sont relativement faibles, il est fréquent d'obtenir des résultats en fonction des heures avec ure dispersion telle qu'il serait tentant de conclure à une apparition aléatoire des incidents, alors que si l'on raisonne selon une autre échelle de vieillissement, il est possible de dégager une loi d'usure.

Le fichier actuel ATAR ne compórte que peu de paramètres relatifs aux conditions d'utilisation propres à chaque vol, mais pour d'autres matériels, il est prévu de décomposer les temps de vol selon les différentes phases d'utilisation (montée, subsonique, supersonique, post-combustion, etc...) ou de les compléter par un nombre de manoeuvres.

C'est ainsi que le taux de pannes d'un démarreur ne peut être ramené uniquement au nombre d'heures d'activité mais au nombre de missions effectuées et annulées, la fatigue du système résultant à la fois du nombre de manoeuvres faites et du temps de présence sur avion.

De même, une pièce peut avoir plusieurs espérances de durées de vie "en heures" selon qu'elle est utilisée sur un type d'avion faisant des vols longs à haute altitude ou des vols courts, grande vitesse, basse altitude.

.../...

Résultats :

Parmi les travaux standards donnés en annexe, certains se rapportent plus particulièrement à l'objet de cette réunion "la Sécurité".

C'est ainsi qu'il est possible notamment, connaissant :

- le parc total d'un type de pièce, c'est-à-dire pour chaque pièce produite, son affectation et ses antécédents

Retrait des pièces dangereuses.

de retirer du service toutes celles qui présentent un caractère quelconque affectant la sécurité (temps de fonctionnement, date de fabrication, condition d'utilisation, etc...).

Ex : aubes de turbine du N° de coulée 2 512 âgées de plus de x h depuis fabrication.

En plus de la Sécurité, il est possible d'étudier :

. Les répercussions industrielles : cadencement de livraison des pièces de remplacement.

. Les répercussions opérationnelles : nombre d'interventions à faire par le Client - nombre de moteurs indisponibles.

Caractéristiques de fiabilité.

Connaissant à la fois en fonction du vieillissement,

- les matériels en cours de service ou reconnus bons après examen,

- les matériels retirés du service pour avarie ou mauvais fonctionnement, soit pour les rebuter, soit pour les réparer,

il est possible de calculer le taux d'avarie correspondant $\frac{\text{nombre de matériels avariés}}{\text{nombre de matériels exposés}}$, d'en étudier les variations.

Ensuite, il est calculé et tracé, selon la méthode actuarielle, une courbe de survie dont il est déduit une courbe d'endurance moyenne qui donne l'espérance mathématique du nombre d'unités de vieillissement qui seront accomplies en moyenne par un matériel, compte tenu de son vieillissement et des déposes prématurées.

.../...

Influence des conditions d'entretien :

Pour l'étude du taux d'avarie, il est important de distinguer les pièces dont le mauvais fonctionnement ou l'avarie se manifeste immédiatement, de celles dont tout défaut ne peut être détecté qu'à l'occasion d'un contrôle périodique.

Pour les matériels entretenus selon la méthode dite de Maintenance préventive, le point "exact" de la détérioration ou de la baisse de performance n'est pas connu puisque la dépose d'un matériel se situe souvent, soit en avance par rapport à ce point de détérioration critique, soit après dépassement des critères admissibles depuis un laps de temps inconnu.

Ceci pourrait donc être un point de départ pour déterminer parmi les pièces ne mettant pas directement la sécurité en jeu :

- celles qui doivent être suivies de façon continue pour éviter un nombre de déposes abusif

et,

- celles qui sont toujours justiciables de l'entretien préventif, cette distinction étant fonction de la dispersion de la durée de vie de la pièce.

Maintenance continue.

Pour une connaissance plus rapide et plus précise de la fiabilité des matériels, les nouvelles techniques de Maintenance envisagées semblent offrir de nombreux avantages.

Par exemple, il serait idéal de fixer des seuils d'alarme permettant d'assurer une fiabilité suffisante pour une unité de fonctionnement qui serait alors la durée d'un vol au lieu de la durée séparant deux visites périodiques.

Mais ceci pourrait conduire à immobiliser fréquemment le moteur et à des déposes non groupées des ensembles ce qui irait partiellement à l'encontre du but recherché : améliorer la sécurité, certes, mais réduire par ailleurs le coût d'entretien.

.../...

L'analyse de l'évolution des défauts et de divers paramètres permettra alors de fixer de nouvelles valeurs de seuils d'alarme et de nouvelles lois de Maintenance.

Par exemple :

. définir certaines limites de potentiel au-delà desquelles les risques d'avarie s'accroissent anormalement sans être compensés par un gain substantiel d'endurance moyenne,

. élargir la périodicité d'examen en adaptant les critères d'admissibilité des défauts.

Par ailleurs, l'étude des interactions entre certains paramètres pourra limiter ultérieurement la détection à leur résultante ou au paramètre prédominant.

L'enregistrement en vol de la valeur de certains paramètres pourra également renseigner de façon plus rapide et plus précise, non seulement sur la constatation de la défaillance elle-même, mais aussi sur l'origine des défaillances.

C'est ainsi qu'au lieu de constater une détérioration de roulement et d'attendre les résultats d'une expertise plus ou moins longue et difficile, cette détérioration pourra être analysée en liaison avec d'autres dépouillements définissant les conditions d'emploi : température, pression, niveau vibratoire, etc...

Les travaux statistiques pourront faire apprécier :

- si la défaillance est la conséquence des conditions anormales d'emploi (dans ce cas une modification n'est pas à envisager pour la pièce endommagée mais pour un circuit de graissage, par exemple),

ou,

- si cette défaillance est imputable à la conception de la pièce et risque de se reproduire, alors l'étude d'une modification doit être entreprise.

Cette modification peut avoir pour objectif, soit une augmentation de la durée de vie, soit l'amélioration du taux de défaillance. Toutefois, ces deux actions ne peuvent être totalement indépendantes car le recul de la période d'usure est complètement inutile si le taux de défaillance reste médiocre.

Là encore, ce sont les courbes de survie qui renseigneront sur le sens des modifications à entreprendre.

Il sera donc possible, avec des informations nombreuses, progressives et les moyens correspondants de dépouillement et de calcul :

- de constituer des classes de pièces pouvant être examinées ou déposées simultanément sans perdre un nombre d'heures important d'utilisation,
- d'élaborer des modifications de telle sorte qu'elles assimilent une pièce à une classe telle qu'il ne lui soit pas attribué des avantages superflus et inutilisés compte tenu des fiabilités amont et aval.

Il va de soi que tous ces résultats permettront en outre de construire un système logistique rationnel, dont l'évaluation du coût pourra tendre vers un optimum en fonction des services demandés.

BUTS	TRAVAUX PRINCIPAUX
A - Technique	1°) - Relevé des incidents exploitation et réparation - par catégorie - par importance en fonction de : - standard des pièces - circonstances et conditions d'utilisation - cycles/temps de fonctionnement
	2°) - Taux/1000 heures par Cie) pour une période de global) temps ou en cumul
	3°) - Répercussion des modifications.
B - Opérationnel	1°) - Calculs et tracés des fréquences et répartitions des contrôles et interventions de dépannage - programmés - non programmés
	2°) - Etudes des pourcentages des déposes - justifiées - injustifiées
	3°) - Analyse des durées des interventions des immobilisations ou retard par catégorie de pièces " d'incident
C - Economique	1°) - Taux de mise en réparation en révision générale (programmée (non programmée en rebut
	2°) - Taux d'interventions et réparations sous-garantie hors-garantie

D - Statistiques

Création pour un certain nombre de pièces importantes d'un état de service mécanographique permettant de connaître intégralement périodiquement

- l'état
- la position
- le standard
- le vieillissement

de chacune des pièces fabriquées.

E - Fiabilité

Compte-tenu des travaux réalisés pour A, B, C et des informations contenues en D,
établissement des caractéristiques de fiabilité

- probabilité de survie
- taux avarie
- endurance moyenne

(méthode actuarielle)

F - Logistique

Simulation et prévision du nombre d'interventions et des volants nécessaires correspondant à un type d'exploitation défini (type de vol, nombre d'heures d'exploitation, temps de rotation journalier, cycle de réparation, etc...).

Organigramme du Circuit de l'Information « Réacteurs ATAR »

DESIGNATIONS DES CODES CARTE	*	@	A	B	D	E·F·G	H·I·J	K·L	M·N..
INFORMATION CONCERNEE	FABRICATION	MONTAGE	ASSEMBLAGE	ESSAIS	INTERVENTIONS REP - REC MODIFICATION	UTILISATION	EXPERTISE	PROTOCOLE de REPARATION	EXAMEN en USINE
SERVICES RESPONSABLES	CG · CL	CL · CB HC · AIA	CL · CW AIA	CW · AIA	CG·CL·CB CW·HC AIA	MCI CW	CDE	CW· CB HC · AIA	CB·HC AIA

Collecte

Traitement

Exploitation

- documents de base
- cartes
- bandes magnétiques

ORDINATEUR (AGO)

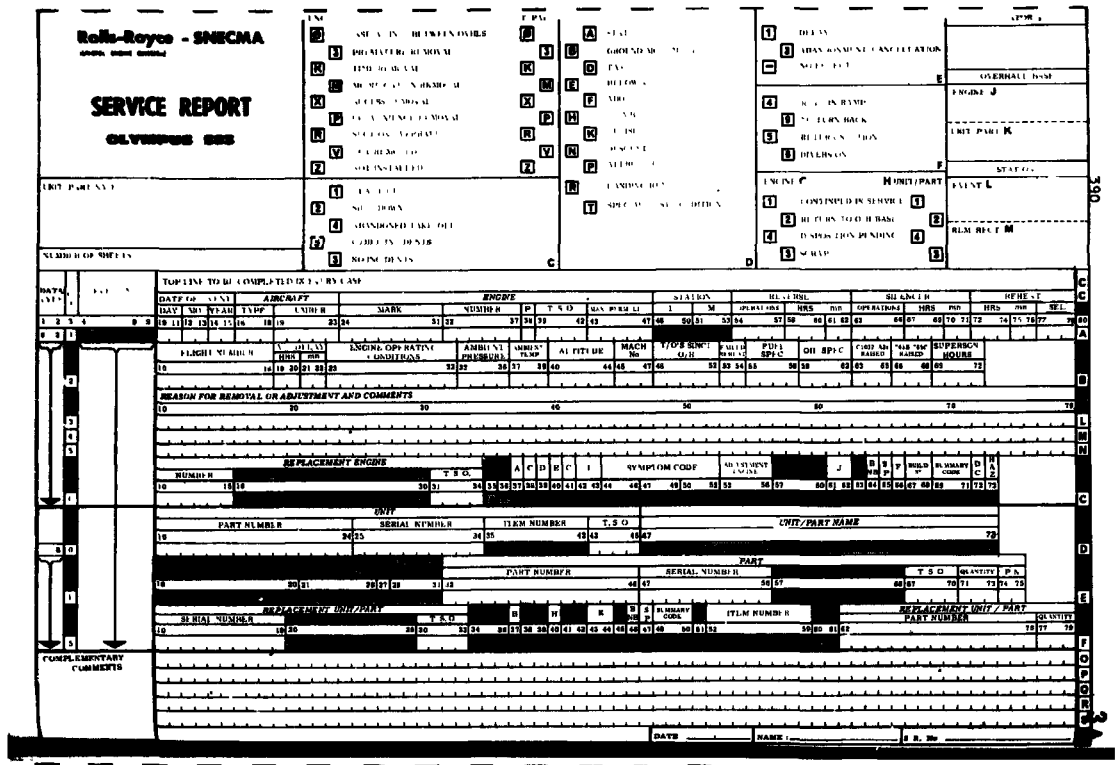
- listings - microfilms
- affichage sur écran

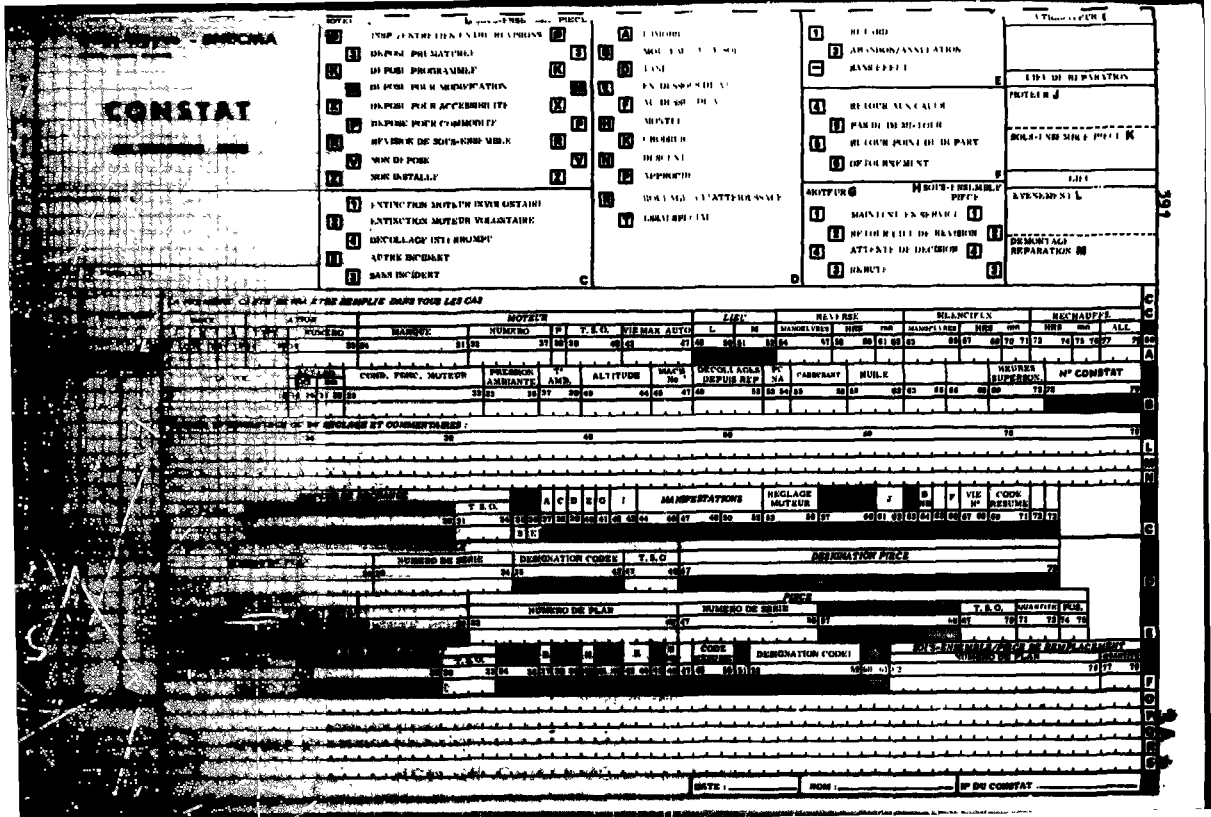
STATISTIQUES

Synthèses

listings

DIRECTION Exploitation	DIRECTION Technique	DIRECTION des Contrats	Chargés de Mission	Services Officiels	DIRECTION du Controle	
MC-MT-MR	tous services Y	SV - RFV	SM	STAé-SIAR SPAé	tous services CD - CB	MCI - HC AIA


Rolls-Royce - SNECMA
SERVICE REPORT
OLYMPUS 593
UNIT PART NO. K
NUMBER OF SHEETS
ENGINE J
OVERHAUL DATE
STATUS
EVENT L
REMOVED M
TOP LINE TO BE COMPLETED IN EVERY CASE
AIRCRAFT
ENGINE
STATION
REMOVAL
SUBSEQUENT
REMOVAL
DATE OF EVENT
TYPE
NUMBER
MARK
NUMBER
TSO
FLIGHT NUMBER
ENGINE OPERATING CONDITIONS
AMBIENT PRESSURE
AMBIENT TEMP
ALTITUDE
MACH No
T/O'S SINCE O/H
FUEL SPEC
OIL SPEC
SUPERSON HOURS
REASON FOR REMOVAL OR ADJUSTMENT AND COMMENTS
REPLACEMENT ENGINE
SYMPTOM CODE
ADJUSTMENT CODE
SUMMARY CODE
UNIT
PART NUMBER
SERIAL NUMBER
ITEM NUMBER
UNIT/PART NAME
PART
QUANTITY
REPLACEMENT UNIT/PART
COMPLEMENTARY COMMENTS
DATE
NAME
S. R. No.


CONSTAT
MOTEUR
LIEU
REMPLACEMENT
DEPANNAGE
DEMONTAGE
REPARATION
PIECE
DESIGNATION PIECE
NUMERO DE SERIE
NUMERO DE PLAN
DESIGNATION CODE
MANIFESTATIONS
REGLAGE MOTEUR
DATE :
NOM :
N° DU CONSTAT

FICHIER CENTRAL — CRÉATION

CARTE K : A REMPLIR SYSTÉMATIQUEMENT A CHAQUE RETOUR USINE
POUR TOUT ÉLÉMENT SUIVI PAR LE FICHIER CENTRAL

CARTES M : A REMPLIR DANS LES CAS SUIVANTS { 1 - DÉFAUT NOUVEAU
2 - DÉFAUT HORS CRITÈRES
3 - REBUT

S.N.E.C.M.A. S^de ..... à M.C.I.
DATE : . . . . . .

392

RESERVE	N° ORDINATEUR	DÉSIGNATION EN CLAIR ABRÉGÉE ET LOT POUR LES AUBES	DÉSIGNATION CODÉE	N° PLAN, ÉTAT, INDICE (NORME S.N.E.C.M.A.)	N° INDIVIDUEL	POSITION	TEMPS TOTAL DEPUIS FABRICATION	PÉRIODE	STADE D'EXAMEN	DÉCOLLEMENT DÉVERRAGE (@)		PLEINS (@)	TWISTAGE (@)	MESURE PRISE	SUPPORT (@)		DATE (@)
										CODE GÉNÉRAL (+)	FISSURE (+)	CODE DÉFAUT (+)	IMPORT^ce (+)		LOCAL (+)	REMÈDES (+)	ANCIENNETÉ (+)

393

CARTE D
MODIFICATION - REPARATION
RECUPERATION C. M. S
DEROGATION

3C

S.N.E.C.M.A. S^CO_____ à M.C.I.
DATE : .....

FICHIER CENTRAL — CREATION

CARTE D A REMPLIR DANS LES CAS SUIVANTS :

MODIFICATION, AMENDEMENT
REPARATION (REP. INSTRUCTION)
RECUPERATION
C. M. S. (CONSIGNE DE MISE AU STANDARD)
DEROGATION

Pour tous les éléments suivis au fichier central

CODE DE CARTE : D 1

EMETTEUR 2

DESIGNATION EN CLAIR ABREGEE
PLUS LE LOT POUR LES AUBES 3 11

DESIGNATION CODEE 12 18

N° PLAN, ETAT, INDICE : 19 31

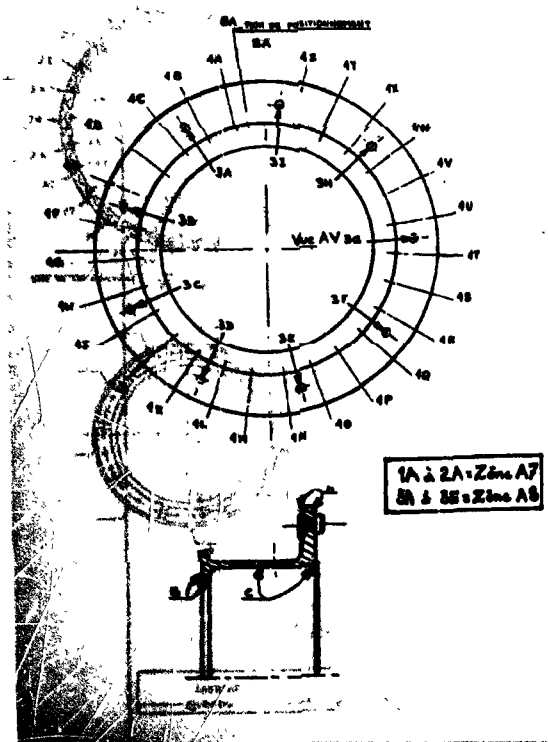
N° INDIVIDUEL
SOUS-LOT PLUS ORDRE POUR LES AUBES 32 39

*

45 DATE D'APPLICATION	46 47 LIEU	48 A PLA. DEMEURE	49 50 TEMPS TOTAL DEPUIS FABRICAT	55 56 OPTION	57 INTERVENSION NUMERO	70 rev	typ	71	73	74 NUMERO MOTEUR	78	79 80 REMARQUES CODIFIEES

Exemples :	Numéro										Rév.	Type	CMS	Alinéa
Modificateur, révisé, paragraphe, alinéa						5	4	1	0		2	M	1	5
						5	4	9	3		2	M	2	B
Répertoire de Modif., annexe, paragraphe					1	4	5	8	2	2	1	2	T	3	
REP, indice							3	6	5	4		3	P		
Instruction de révision provisoire, paragraphe, alinéa							6	1	7	6			N	A	2
Instruction de révision) groupe, sous-groupe, pièce, opération			*			1		1		E			F	2	
paragraphe (ou figure)			8			2		1		A			F	3	
		1	1			8		3	1	8			F		
		1	1			1				2			F		
Demande de récupération, catégorie						1	8	1	2	8	1	A	C		
Plan modificatif, indice	4	8	5	7	2	8	0	3	3			4	P		
Récupération, indice						1	2	1	3			2	R		
CMS, révision								1	9			3	S		
Dérogation								2	5				D		

Groupe 6	Sous-groupe 7	EDITION N°
TURBINE	ANNEAU 1er ETAGE	9K

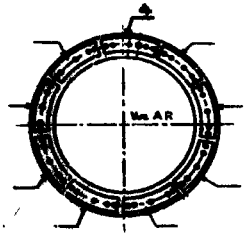


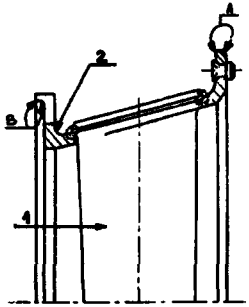
EDITION N°	Groupe 6	Sous groupe 7
9K	TURBINE	ANNEAU 1er ETAGE

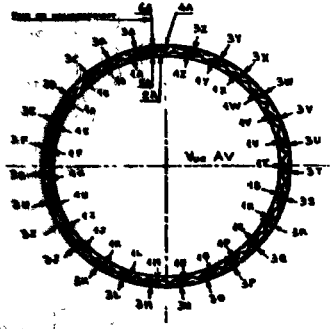
DÉSIGNATION					G	S/G	OPÉRAT.	QUALIF.	PRIORITÉ
AN	N	TV	A		6	7			4

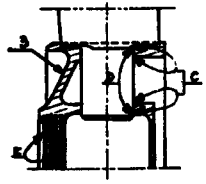
Groupe 6	Sous-groupe 6
TURBINE	REDRESSEUR

EDITION N° 0
9K









3A à 4A = Z8 = A6
1A à 2A = Z8 = A7
sens voir 9A 3

EDITION N°
9K

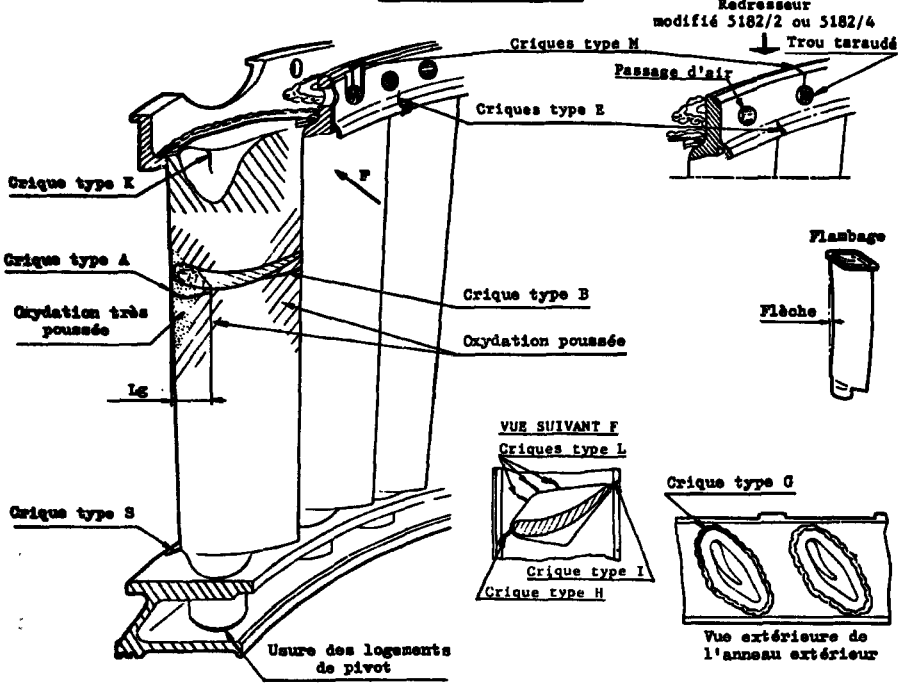
Groupe 6	Sous-groupe 6
TURBINE	REDRESSEUR

DÉSIGNATION	G	S/G	NOMBRE	NOMBRE	REPÈRE	
REDR TU		6	6			0
AVB REDTU		6	6		1	M
ANN EXT		6	6		2	N
ANN INT		6	6		3	P
LECHETTE		6	6		4	Q

(à coder par quantité).

5.53

REDRESSEUR DE TURBINE



CONTROLE DU REDRESSEUR DE TURBINE
Mise à jour - 15 FEVRIER 1968

A DESCRIPTION OF THE

AIR CANADA

UNIT QUALITY RECORD

A. I. R. SYSTEM II

Supplied by K.E. Chapman,
Director, Maintenance Engineering
Air Canada Base
Montreal, Canada

for Meeting of Specialists on the Reliability of Mechanical Systems and Components for Nuclear Reactor Safety,
RISØ, Denmark
24 - 26 September, 1969

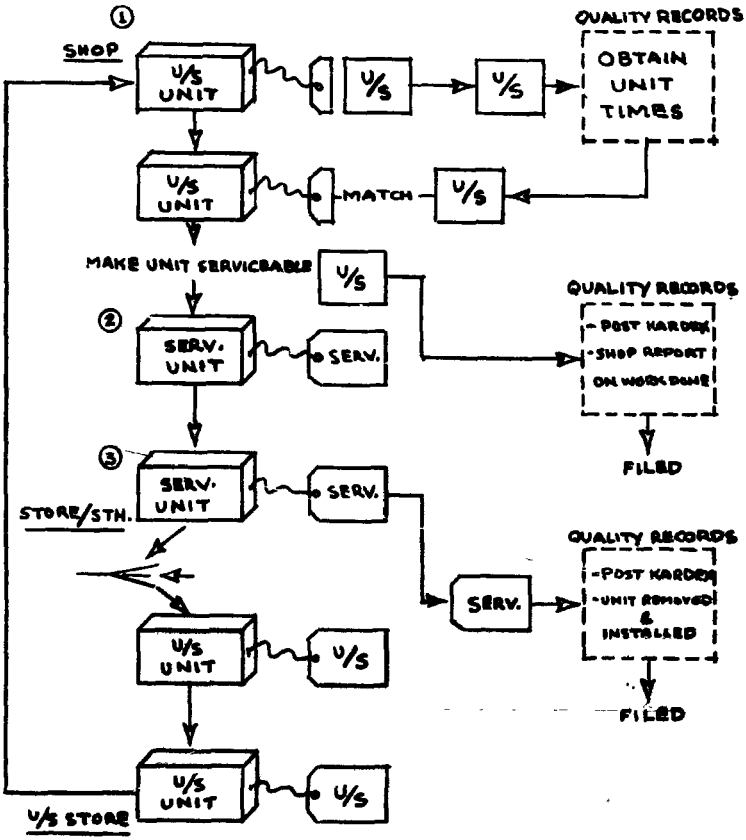
(Mr. Chapman would like to point out that this paper should be considered as an outline only).

OBJECTIVES OF UNIT RECORD SYSTEM

- REAL TIME - LIFE CONTROL OF UNITS
- PERMANENT LEGAL RECORD - D.O.T. REQUIREMENTS
- OFF LINE - INVESTIGATION, PERFORMANCE MONITORING
- CONTROL OF WORK DONE ON UNITS

ABILITY TO MEET OBJECTIVES AFFECTED BY

- GROWTH IN NUMBER OF UNITS CONTROLLED
- CONSTANT STAFF LEVEL
- INCREASED SPEED UNIT CYCLE



PRESENT UNIT RECALL SYSTEM

PRESENT SYSTEM FLOW CHART

DESCRIPTION OF PRESENT SYSTEM FLOW CHART

1. A U/S tag is already attached to the unserviceable(U/S) unit when it is received in the shop for repair, check or overhaul.

   The bottom portion of this tag which contains unit number, description, reason for removal, etc. is sent to QUALITY RECORDS DEPT. (Q/R).

   Information on the U/S tag is checked against the unit record card (KARDEX) which is a permanent record of the unit life cycle, A/C on, A/C off, dates, times, etc. ....

   Unit times are computed and written on the tag which is sent back to the shop.

2. On the back of this tag the Shop Mechanics enter repair information, modification done, components replaced, etc. This tag is then sent to Q/R for final posting on KARDEX.

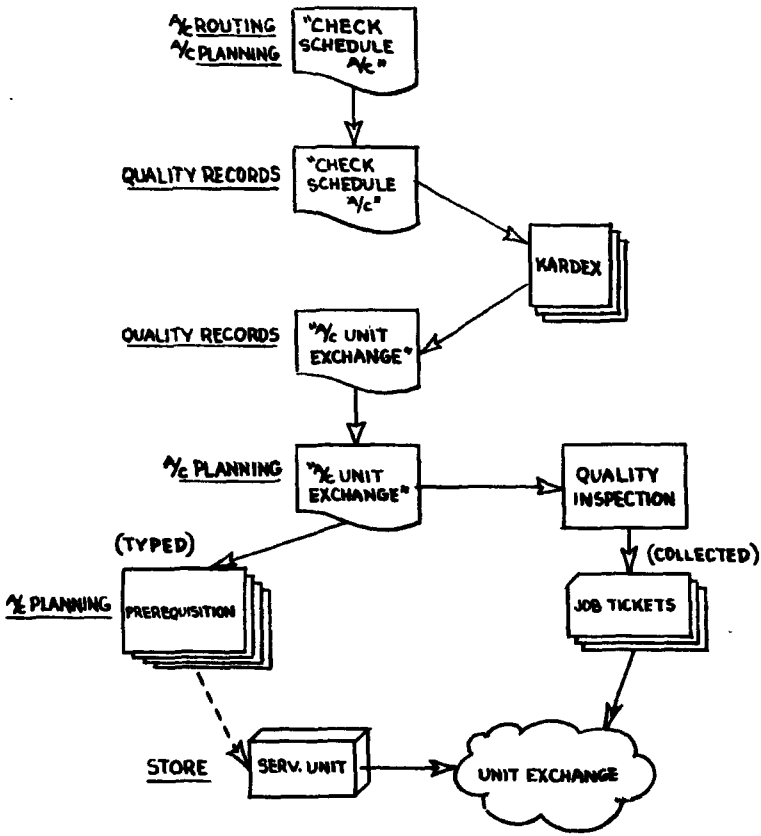
   A serviceable tag is prepared (unit number, description, etc.) and attached to the unit to identify it as a serviceable unit.

3. When a unit is installed on A/C the installation information of this unit and removal information of the corresponding unit is written on the serviceable tag and sent to Q/R.

   When it is received in Q/R this tag is used for posting on corresponding unit KARDEX.

   A U/S tag is prepared for the unit which is removed and attached on unit removed.

   The unit is sent to U/S Stores and then to the shop, where the cycle is restarted.



PRESENT UNIT RECALL SYSTEM

DESCRIPTION OF PRESENT UNIT RECALL SYSTEM (FLOW-CHART)

- A "CHECK SCHEDULE A/C LIST" is issued once a week by PLANNING & ROUTING, giving the A/C No. and the date of its next visit (MOC, AV, O'haul). The list covers all Aircraft visits for the following four weeks.

- On receiving this list Q/R check every unit KARDEX for each scheduled A/C for: time expired units, planned sampling units, etc. ....

- For each A/C visit a list of units to be exchanged is prepared and sent to PLANNING & QUALITY INSPECTION.

- From this list QUALITY INSPECTION collect job tickets for this A/C visit.

- PREREQUISITIONS are typed from this list and sent to Stores. The units are then grouped in Stores and sent to the hangar for the scheduled visit of the A/C.

DESIGN OBJECTIVES

- CAPTURING BASIC DATA AS CLOSE TO SOURCE AS POSSIBLE
- MINIMIZE PAPER FLOW
- AUTOMATE ALL ROUTINE OPERATIONS
- HUMAN AUDIT BY EXCEPTION
- ENLARGED INFORMATION RETRIEVAL SERVICE

PROPOSED SYSTEM FLOW CHART

NEW SOURCE DOCUMENTS - THREE PART TAG

1 **Shop Report**

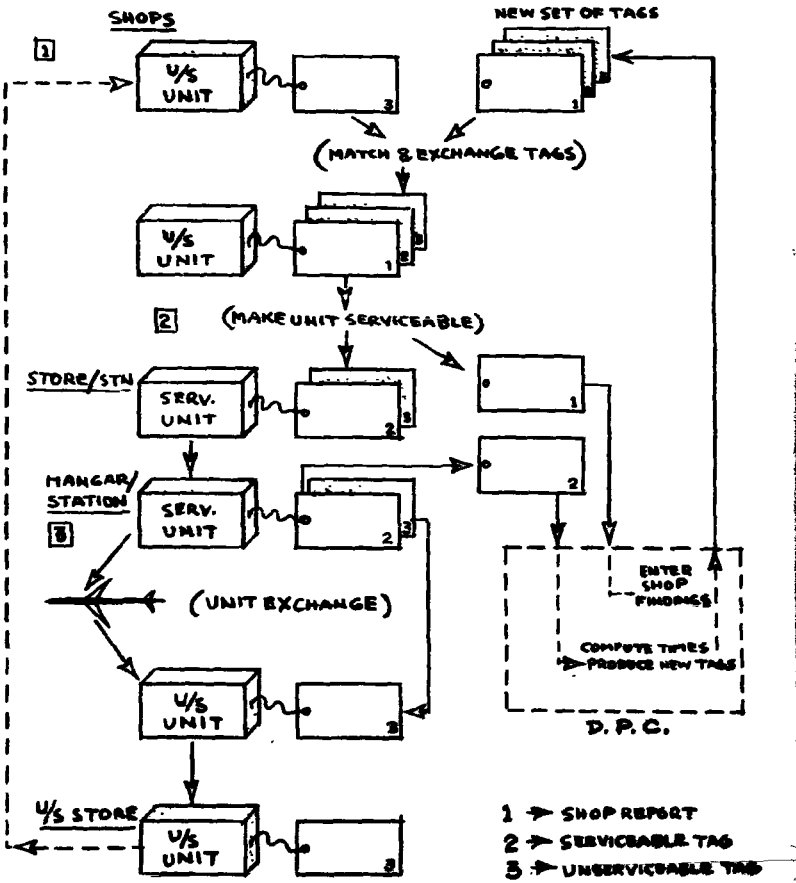
- USED TO REPORT WORK DONE ON UNIT
- 35% OF ENTRIES PREPRINTED (COMPUTER)
- WRITTEN IN SHOPS ONLY
- CONTAINS PLANNED SAMPLING INFORMATION (WHEN APPLICABLE)

2 **Serviceable**

- USED TO IDENTIFY SERVICEABLE UNITS
- 30% OF ENTRIES PREPRINTED (FROM ABOVE TAG)
- WRITTEN IN HANGAR & STATION ONLY
- CONTAINS INSTALLATION & REMOVAL INFORMATION

3 **Unserviceable**

- USED TO IDENTIFY UNSERVICEABLE UNITS
- NO WRITING REQUIRED ON THIS TAG
- CONTAINS REMOVAL INFORMATION ONLY



PROPOSED SYSTEM FLOW CHART

DESCRIPTION OF PROPOSED SYSTEM FLOW CHART

1. - A U/S tag is already attached to the unserviceable (U/S) unit when received in the shop for repair or check and contains all removal information.

   - Prior to that, a new three part tag has been prepared on computer and received in the shop (see new source document).

2. - Shop report (first copy of the new tag) is filled in by the Mechanic, detached and sent to update the computer files. The shop enters information on only this portion of the tag. The old U/S tag is then filed.

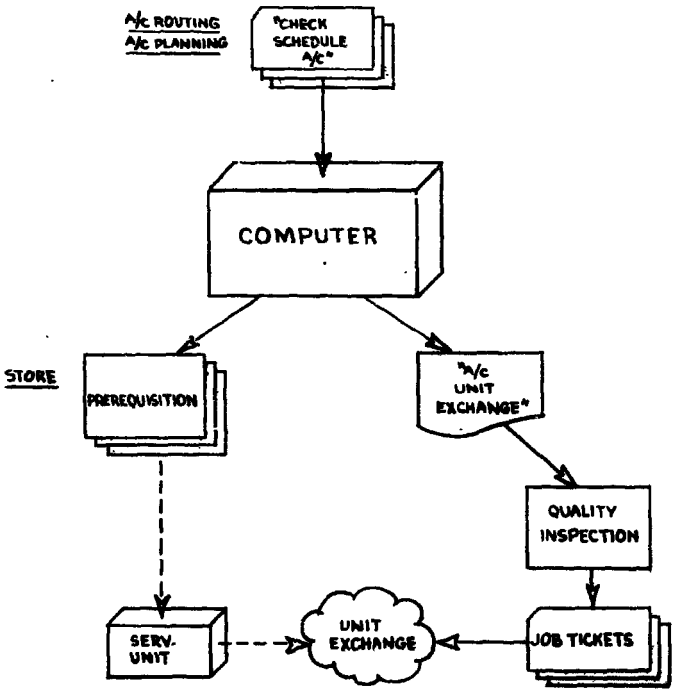
   - The new tag (two parts left) is attached to the unit. The serviceable tag (top part of new tag) identifies the serviceable unit.

3. - When this serviceable unit is installed on the aircraft and the corresponding one removed, both removal and installation information is written on this tag.

   - When completed, the top part of this tag is detached and sent to update computer files. This will generate a new three part tag for the unit removed.

   - The last part of the tag (carbon copy of the second one) is attached to the U/S unit (no writing required on this portion).

   - The unit is sent to Stores and then to the shop (the cycle continues as in (1)).



PROPOSED UNIT RECALL SYSTEM

DATA PROCESSING FLOW CHART

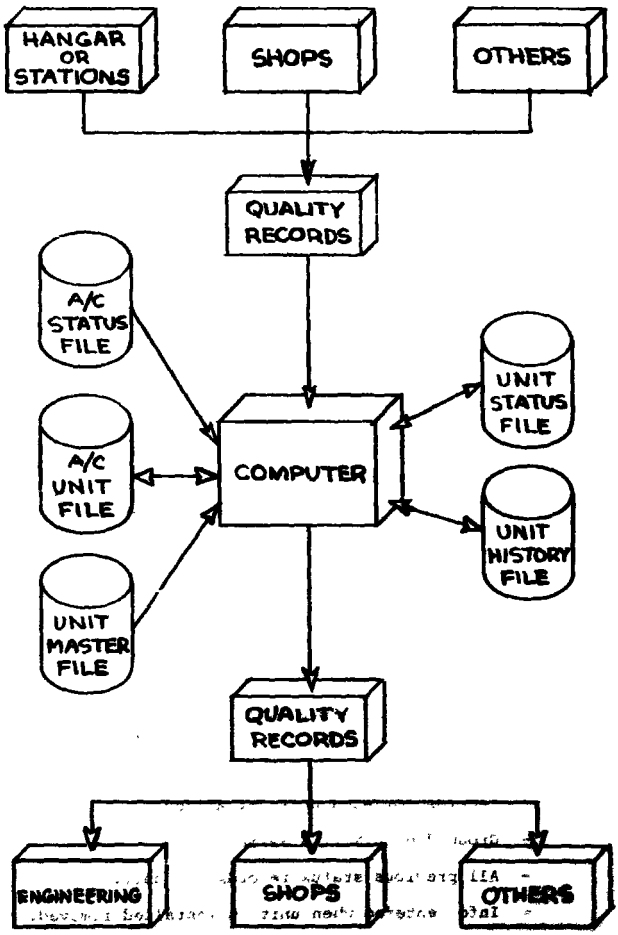
DESCRIPTION OF PROPOSED UNIT RECALL SYSTEM

- A predetermined number of days prior to a scheduled aircraft visit, a card is prepared for this A/C, giving the type and expected date of visit.

- The program will calculate unit times and prepare a list of the unit exchanges required.

- For each unit exchange called, a prerequisition will be prepared and sent to Stores.

- The A/C unit exchange list printed will be sent to Quality Inspection.



DATA PROCESSING FLOW CHART

DESCRIPTION OF COMPUTER FILES

A/C STATUS FILE

- One record for each A/C
- A.C.T.I.O.N. generated info. on A/C hrs, cycles, landing ....

UNIT MASTER FILE

- One record for U.N.I.
- Contains identification, description, control, limits.

A/C UNIT FILE

- One record for each U.N.I. on A/C
- Grouped by A/C No.
- Installation info.

UNIT STATUS FILE

- One record for each unit serialized.
- Grouped by U.N.I.
- Current status.
- Installation/removal/shop info.

UNIT HISTORY FILE

- Records for each unit serialized.
- Grouped by U.N.I. & Serial No.
- All previous status records for unit.
- Info. entered when unit is installed/removed.

DATA PROCESSING FLOW CHART

BENEFITS OF A.I.R. SYSTEM II

TO: SHOP - A/C & LINE MECHANICS

REVISED DATA COLLECTION

- REDUCE WRITING BY 50% - 60% (ENTRY)
  - ONE TAG (NO DUPLICATION)
  - NUMBER OF ENTRIES (PREPRINTED INFO.)
- SPEED UP PAPER FLOW
  - TAG RECEIVED BEFORE UNIT
  - UNIT TIMES (PREPRINTED)
  - FULL TAG STAYS WITH THE UNIT

BENEFITS OF A.I.R. SYSTEM II (cont'd)

TO: QUALITY RECORDS - A/C PLANNING & WAREHOUSE

UNIT RECALL

- ELIMINATE MANUAL CHECK FOR UNIT RECALLS
  - PRODUCED BY COMPUTER
- ELIMINATE TYPING OF PREREQUISITIONS
  - PRODUCED BY COMPUTER
- REDUCE FALSE UNIT RECALLS
  (BY COMPRESSING INTERVAL BETWEEN RECALL & A/C ARRIVAL)
  - MOVEMENT OF UNIT FROM WAREHOUSE TO HANGAR
  - PREPARATION OF JOB TICKETS
  - CHECK FOR PRESENCE OF UNIT ON A/C (MECHANIC)
  - PRODUCTION REQUEST ON THE SHOP

BENEFITS OF A.I.R. SYSTEM II (cont'd)

TO: QUALITY RECORDS

AUTOMATION OF RECORDS

- AUTOMATED RECORDING AND AUDITING

  TIME AVAILABLE FOR:

  - AUDIT OF SYSTEM, CHECKING OF EXCEPTION, PROVIDING INFORMATION

- INCREASE SPEED OF INFORMATION FLOW

  - RECORDS MORE UP-TO-DATE

- EFFICIENT & TIMELY REPORTING

  - ROUTINE REPORTS
  - INDIVIDUAL INQUIRIES
  - ON REQUEST SURVEYS

DATA PROCESSING REQUIREMENTS

CONVERSION OF EXISTING RECORDS:

MOHAWK DATA RECORDER - OPERATED BY INDEX CLERK

- 1 RECORDER/1 CLERK - $600/MONTH

TOTAL : $10,000

ROUTINE OPERATING SYSTEM:

INPUT PREPARATION - KEYPUNCHING OR DATA RECORDER

- 500 DOCUMENTS/DAY - $400/MONTH

BATCH PROCESSING - RANDOM ACCESS UPDATING

- OUTPUT REPORTS

- .50 HOUR/DAY - $2,600/MONTH

TOTAL - $3,000/MONTH

ON-LINE INQUIRIES (IMMEDIATE RESPONSE)

DAY SHIFT ONLY

- ONE DISC DRIVE - $800/MONTH
- INQUIRY TERMINAL - $400/MONTH

TOTAL: $1,200/MONTH

PROPOSED SCHEDULE

	START DATE	COMPLETION DATE
DETAILED DESIGN	DEC/67	MAY/68
PROGRAMMING/TESTING	APRIL/68	SEPT/68
TYPE TRIAL OF SYSTEM	SEPT/68	DEC/68
IMPLEMENTATION	JAN/69	

PROJECT TEAMS

DETAIL DESIGN TEAM

(Full Time)

- Quality Records	:	M. Morrison
- Data Processing	:	R. Valois G. Langevin
- Management Systems	:	A. Laferriere

COORDINATING TEAM

- A/C Maintenance	:	J. McArton
- Line Maintenance	:	W. Fairbairn
- Engineering	:	G. Haigh
- Planning	:	T. Murray
- Quality	:	P. Brown
- Management Systems	:	A. Bodnarchuk P. Jeanniot

A REVIEW AND DISCUSSION OF METHODS AND TECHNIQUES OF ACQUIRING, DISSEMINATING, EXCHANGING, AND UTILIZING TEST DATA AND FAILURE RATE DATA ON PARTS/COMPONENTS ON A NATION-WIDE BASIS

by

Stanley I. Pollock

Naval Fleet Missile Systems
Analysis & Evaluation Group,
Corona, California

ABSTRACT

This paper provides information on how to enhance the disciplines of reliability, safety, maintainability, and systems effectiveness by utilizing data pertaining to parts/components, which are acquired, disseminated, and exchanged through the media of two nationally known and recognized data exchange programs:

Interagency Data Exchange Program (IDEP),

Failure Rate Data (FARADA) Program.

INTRODUCTION

The Naval Fleet Missile Systems Analysis and Evaluation Group (FMSAEG) located at Corona, California, has been assigned the task of conducting program management on behalf of the Navy for the Interagency Data Exchange Program (IDEP) and on behalf of all the Services and NASA for the Failure Rate Data (FARADA) Program.

To have some appreciation of the need for the data being exchanged in these programs, one must consider the requirements of a contractor engaged in the design, development, and production of a missile or an aerospace subsystem or equipment. It is during the design and development phase of a project that the engineers (at a contractor's plant) who are responsible for the reliability, safety, maintainability, and effectiveness of these subsystems and equipments have an urgent need for considerable amounts of technical data including information on parts/components (electrical, electronic, mechanical, hydraulic, pneumatic) intended for use in the equipment they are designing. This information covers a wide spectrum--for example, who manufactures the part/component; who purchases them; why they were purchased, i.e., for what program and for what intended use; who tests them; what were the results of tests (such as qualification tests, evaluation tests, engineering and environmental tests), and what was the "use-history" of these parts/components when placed in operation and subjected to actual operating environments. And last, but not least, is the need for information on failure rates of these parts/components, which entails knowledge of quantity used, quantity failed, operating time or cycles to failure, and for other data including causes of failure, modes of failure, and operating stresses at time of failure.

The objective is, specifically, how to make all this information readily available and useful to the engineers who have need of this information; this objective has been achieved by these two data exchange programs.

ORIGIN AND GROWTH OF DATA EXCHANGE PROGRAMS

Both IDEP and FARADA originated--or were created--to fill the specific needs of the design engineers. However, they were not created instantaneously nor by edict. They had their origin many years ago (1957-1958) as a small task assignment to FMSAEG. The substance of the assignment was to provide the design engineers who were engaged in the POLARIS (missile) program with all the available essential information on parts/components. The schedule that was established for the POLARIS program simply did not afford the time for the lengthy--and costly--effort normally expended in purchasing parts/components and subjecting them to the various qualification, environmental, and engineering tests. Instead,

the experience that had been gained or learned in previous missile and aerospace programs was to be imparted to the POLARIS engineers through the acquisition of all sorts of data on the parts/components that had been tentatively selected for use in the POLARIS missile. The objective was to obtain and utilize the most reliable "off the shelf" parts/components available within the constraints of time, funding, and state-of-the-art.

The results of this new approach revealed that many tests could be truncated or eliminated; that a great quantity of hardware for testing need not be purchased: and, finally, that many of the designs on the drawing boards need not be scrapped later in the program due to some deficiency in reliability, safety, maintainability because of the fact that timely and useful information had been provided to the design engineers as soon as it became available. For example, tests conducted on a particular hydraulic device by another contractor for use on another program indicated there were serious problems associated with that device. This information was immediately imparted to the POLARIS design engineers, and as a result they altered an initial design which had incorporated that same hydraulic device.

This early program, conducted by FMSAEG, was identified as the Component Reliability History Survey (CRHS). Between the years 1958-1963, it provided engineers of the prime contractors engaged in the POLARIS effort with much useful information mainly obtained from contractors' test reports generated because of the need for data on other Navy, Army, Air Force projects. This program saved the Navy much time, effort, and money, and the concept and techniques developed to acquire and disseminate data automatically became the basis for the exchange of similar data throughout the entire Navy, as well as the Army, and the Air Force. In fact, the commanders of the ballistic missile agencies of the three Services approved the Interservice Data Exchange Program in 1960. Subsequently, arrangements were made to exchange data with the National Aeronautics and Space Administration (NASA) and the Canadian Military Standards Agency (CAMESA). Thus in 1966, the name of the program was expanded to the Interagency Data Exchange Program (IDEP) and was approved at the level of Assistant Secretary for Research and Development in the three Services and by the Assistant Administrator for Industry Affairs of NASA.

The FARADA Program was a logical outgrowth of IDEP and came into existence in 1961-1962. The specialty of this program is the dissemination of timely data on failure rates and failure modes of parts/components to user participants.

In the beginning, approximately 60 contractors and Government Agencies participated in the data exchange programs. Today, IDEP has 210 participants, and the FARADA Program has 279 participants.

PROGRAM DIRECTION AND SUPPORT

Both programs receive direction from a Policy Board composed of one representative from each of the military services and from NASA. The Board develops and approves Program policies and management procedures for administration.

A Technical Coordinating Committee assists the Policy Board on matters pertaining to FARADA; a Contractors' Advisory Board composed of members selected from the various participants provides information and guidance to the Policy Board relative to the desires of industry for IDEP.

Funds to support these Programs are obtained from the various elements of the three Services and NASA.

MECHANICS OF OPERATION

Both IDEP and FARADA are voluntary in nature, and no fees or assessments are charged to the participants. No classified information is exchanged; neither is company proprietary information divulged.

IDEP

Participants in IDEP submit copies of their purchase specifications, test specifications, and the results of controlled, "laboratory type" tests on electrical, electronic, mechanical, hydraulic, pneumatic parts/components, as well as technical information on materials, production processes, and other data pertaining to the reliability of parts/components, to a designated IDEP office. There are three IDEP offices, one for each of the Services. The Army IDEP office at Huntsville, Alabama, also serves NASA. The Air Force IDEP office is located at El Segundo, California, and the Navy IDEP office is located at FMSAEG, Corona, California. Figures 1 and 2 show the flow of the data.

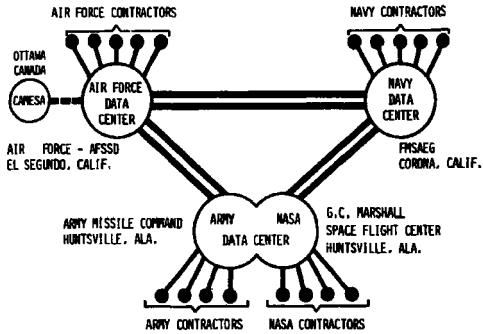


Fig. 1 Interagency Data Flow

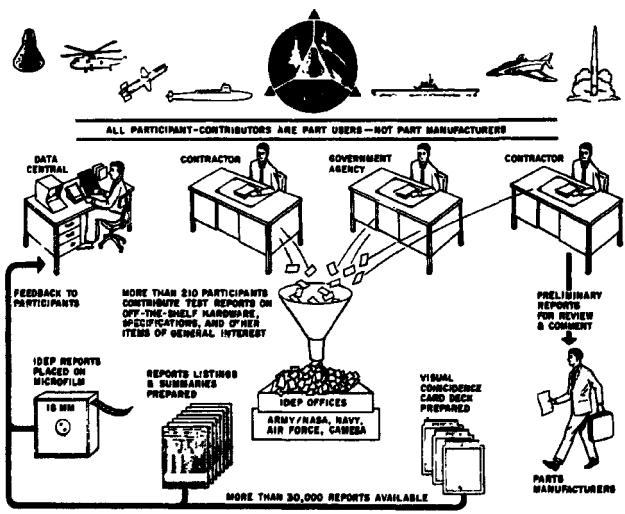
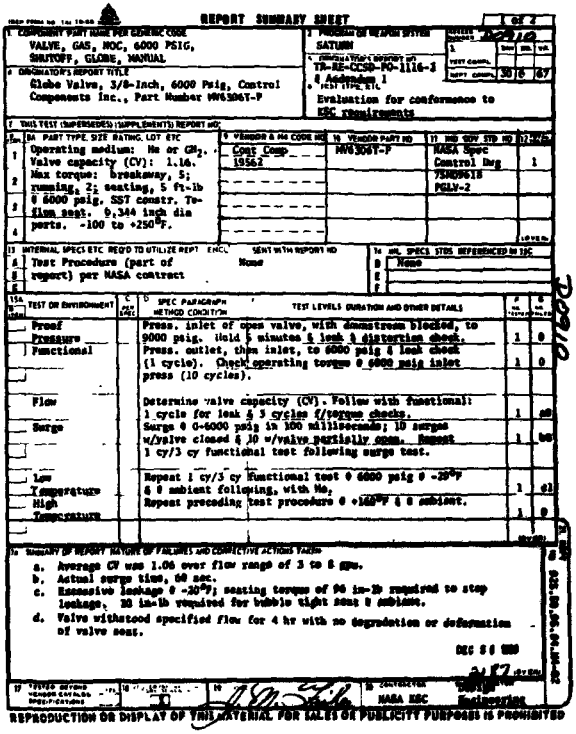


Fig. 2 IDEP Data Flow

A typical IDEP report is illustrated by Figure 3. This report format has been adopted as the standard in IDEP, and the use of this form is required in MIL-STD-831, "Preparation of Test Reports."



REPORT SUMMARY SHEET

1 COMPONENT PART NAME PER CATALOG CODE: VALVE, GAS, NOC, 6000 PSIG, SHUTOFF, GLOBE, MANUAL

2 PROGRAM OR WEAPON SYSTEM: SATURN

3 ORIGINATOR'S REPORT NO: TR-RE-CCSD-PO-1116-3

4 ORIGINATOR'S REPORT TITLE: Globe Valve, 3/8-Inch, 6000 Psig, Control Components Inc., Part Number MW6306T-P

5 TEST CONFIG. 1

6 TEST TYPE, ETC.: Evaluation for conformance to REC requirements

7 THIS TEST (SUPERSEDES) (SUPPLEMENTS) REPORT NO:

No.	8A PART TYPE, SIZE RATING, LOT ETC	9 VENDOR & MFR CODE NO	10 VENDOR PART NO	11 MIL SPEC STD NO	12 NO.
1	Operating medium: N_2 or GH_2. Valve capacity (CV): 1.14. Max torque: breakaway, 5; running, 2; seating, 5 ft-lb @ 6000 psig. SST constr. Teflon seat. 9.344 inch dia ports. -100 to +250°F.	Cont Comp 19562	MW6306T-P	NASA Spec Control Dwg	1
2				TEMPOSEAL	
3				POLY-2	
4					

13 INTERNAL SPECS ETC REQ'D TO UTILIZE REPT (ENCL / SENT WITH REPORT NO):
A Test Procedure (part of report) per NASA contract — None

14 MIL SPECS STDS REFERENCED IN SRC:
D None

15A TEST OR ENVIRONMENT	C PER LEVEL	D SPEC PARAGRAPH METHOD CONDITION	TEST LEVELS DURATION AND OTHER DETAILS	# OF TEST/FAILS
Proof Pressure		Press. inlet of open valve, with downstream blocked, to 9000 psig. Hold 5 minutes & leak & distortion check.		1 / 0
Functional		Press. outlet, then inlet, to 6000 psig & leak check (1 cycle). Check operating torque @ 6000 psig inlet press (10 cycles).		1 / 0
Flow		Determine valve capacity (CV). Follow with functional: 1 cycle for leak & 3 cycles f/torque checks.		1 / 00
Surge		Surge @ 0-6000 psig in 100 milliseconds; 10 surges w/valve closed & 10 w/valve partially open. Repeat 1 cy/3 cy functional test following surge test.		1 / 00
Low Temperature		Repeat 1 cy/3 cy functional test @ 6000 psig @ -250°F & @ ambient following, with N_2.		1 / 01
High Temperature		Repeat preceding test procedure @ +160°F & @ ambient.		1 / 0

16 SUMMARY OF REPORT RESULTS OF FAILURES AND CORRECTIVE ACTIONS TAKEN

a. Average CV was 1.06 over flow range of 3 to 8 gpm.
b. Actual surge time, 60 sec.
c. Excessive leakage @ -250°F; seating torque of 96 in-lb required to stop leakage. 28 in-lb required for bubble tight seat @ ambient.
d. Valve withstood specified flow for 4 hr with no degradation or deformation of valve seat.

17 TYPED NAME, ORGANIZATION, TELEPHONE NO.

18

19

20 CERTIFICATION: NASA REC Engineering

Scale: 3/4

Fig. 3 Standardized Report Summary Card

After processing, the IDEP office provides this information, arranged generically, to all other participants in the form of microfilm in cassettes. Certain data are also placed on visual coincidence cards, to assist those searching for and desirous of retrieving information relative to the effects of various environments upon the part/components. Each card is coded in terms of hardware identification and test parameters.

The placement of data onto microfilm and into cassettes and onto visual coincidence cards is shown by Figure 4.

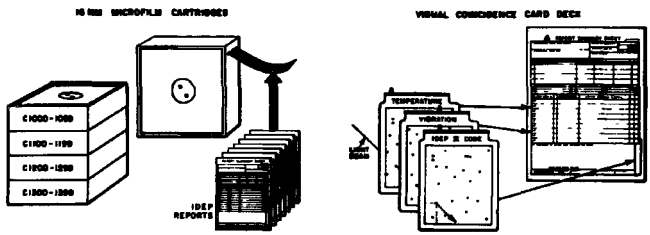


Fig. 4 Placement of Data onto Microfilm and Visual Coincidence Cards

Figure 5 shows a display of visual coincidence cards. A computer listing of IDEP reports (Index of Reports) arranged generically (i.e., a unique nine-digit numbering system) is furnished to all participants on a periodic basis. An extract from such a listing is illustrated by Figure 6. The listing is structured to indicate the cassette containing the microfilmed data desired in order that the cassette may be placed in a microfilm viewer for viewing.

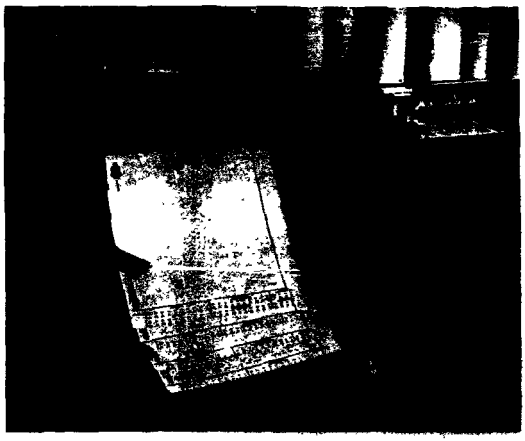


Fig. 5 Display of Visual Coincidence Cards

ACCESS	REPORT NUMBER	ITEM	NOMENCLATURE	VENDOR	PART NUMBER	INVENTORY CODE	DATE	PAGE
	525.00 VALVES, GAS, N.E.C.							
01000	.01.44-P1-005	01	1000-5000 PSIG,CHECK,POP,MANUAL	SPEC,N V			12/64	SATURN
01007	.01.44-P1-00	02	1000-5000 PSIG,CHECK,POP,MANUAL	SNAP TITE	2772-13	ITU	09/00	SATURN
01007	.01.44-P1-05	01	1000-5000 PSIG,CHECK,POP,MANUAL	SNAP TITE	2772-2	ITU	09/00	SATURN
01008	.01.44-P1-005	01	1000-5000 PSIG,CHECK,POP,MANUAL	SPEC,N V			12/66	SATURN
01017	.71.47-P1-155	01	130-1000 PSIG,CHECK,POP,PRESS	SPEC,N V			06/66	APOLLO
01047	.75.47-P1-145	01	130-1000 PSIG,RELIEF,POP,PRESS	SPEC,N V			07/67	APOLLO
01010	.71.47-P1-14	01	100-1000 PSIG,CHECK,POP,PRESS	ACCES PROD	220130-0005	PY	00/00	APOLLO
01016	.71.47-P1-14	02	133-1000 PSI,,CHECK,POP,PRESS	ACCES PROD	220295-0015	PY	00/00	APOLLO
00011	.05.44-N4-03	01	OVER 1000 PSIG,SHUT,GLOBE,MANUAL	ACCES PROD	507211004-134-23	ITU	01/00	SATURN
00457	.05.04-N4-05	01	OVER 5000 PSIG,SHUT,MANUAL	ACCES PROD	533100	IPTU	03/64	SATURN
01106	.70.00-N4-P1	01	100-1000 PSIG	ALCO CONT.	TAC-22HN100	IPU	04/67	SATURN
01107	.70.00-N4-P2	01	100-1000 PSIG	ALCO CONT.	TAC-45HN100	IPU	04/67	SATURN
00259	.03.47-N4-02	01	1500-5000 PSIG,RELIEF,POP,PRESS	AMOSA CORP	2-P528-3	PLPTUV	10/66	SATURN
00909	.05.04-N4-01	01	OVER 1000 PSIG,SHUT,GLOBE,MANUAL	AMRIN CO.	A4425	ITU	03/67	SATURN
01102	.99.04-N4-00	01	OVER 5000 PSIG,SHUT,MANUAL	AUTOCLAVE	20-7183	CRITPTU	04/66	SATURN
01029	.63.46-D7-15	01	0-100 PSIG,RELIEF,POP,PILOT	CALMEC	1031E	IESUV	11/68	SATURN
00774	.66.31-D7-02	01	0-100 PSIG,FLAP,PRESS	CALMEC	511-529	IV	09/68	SATURN
00171	.63.46-D7-13	01	0-100 PSIG,RELIEF,POP,PILOT	CALMEC	519-513	LGTU	06/68	SATURN
00172	.63.46-D7-14	01	0-100 PSIG,RELIEF,POP,PILOT	CALMEC	519-513	U	07/68	SATURN
01111	.05.44-D7-12	01	1350-5000 PSIG,SHUT,POP,SOLEN	CALMEC	838-507C	IDTFT/UUV	09/68	SATURN
01344	.73.44-P1-05	01	100-1000 PSIG,RELIEF,POP,SOLEN	CALMEC	737 - 515	CHTUV	07/68	SATURN
01343	.73.44-P1-04	01	100-1000 PSIG,RELIEF,POP,SOLEN	CALMEC	737-515	UV	04/68	SATURN
01340	.73.44-P1-03	02	100-1000 PSIG,RELIEF,POP,SOLEN	CALMEC	738 - 513	CHTUV	07/68	SATURN
01307	.63.46-D7-16	01	0-100 PSIG,RELIEF,POP,PILOT	CALMEC	931-501	SIUV	10/68	SATURN
00459	.99.04-N4-67	01	OVER 5000 PSIG,SHUT,MANUAL	CAMDAIR	1515-0081	IP	11/65	SATURN
00173	.63.47-D6-01	01	0-150 PSIG,RELIEF,POP,PRESS	CLEVELAND	MS-2532-8	I	04/66	SATURN
00255	.63.47-N4-C2	01	0-150 PSIG,RELIEF,POP,PRESS	CLEVELAND	SK-2023	----	04/66	SATURN
01144	.95.04-N4-19	01	OVER 5000 PSIG,SHUT,MANUAL	CONA PUMP	C-6480	IPTU	05/67	SATURN
01201	.95.04-N4-28	01	OVER 5000 PSIG,SHUT,GLOBE,MANUAL	CONT COMP	MODEL 945	CDIPTU	03/67	SATURN
00910	.99.04-N4-02	01	OVER 5000 PSIG,SHUT,GLOBE,MANUAL	CONT COMP	MVA30AT-P	CDIPTU	04/67	SATURN
01418	.73.47-N4-C1	01	100-1000 PSIG,RELIEF,PRESS	CRANE ASHC	JMC-C TYPE A	IP	03/67	SATURN
00174	.71.17-P1-05	01	100-1000 PSIG,CHECK,BALL,PRESS	FAIRCHLD S	49-1362-91	PT/UV	04/67	SATURN
01202	.93.04-N4-09	01	OVER 5000 PSIG,SHUT,GLOBE,MANUAL	FLOMATICS	MODEL 8610	DIPTU	07/67	SATURN
01019	.99.79-N4-01	01	OVER 5000 PSIG,SHUT,MANUAL,SOLE	FUTURECRAF	2C1644-8-1	IPTU	07/66	SATURN
01108	.05.04-N4-01	05	1000-5000 PSIG,SHUT,MANUAL	FUTURECRAF	3F233	CRITPTUV	0 /65	SATURN
01140	.05.04-N4-01	02	1000-5000 PSIG,SHUT,MANUAL	FUTURECRAF	3G270	CDRITPTUV	A /65	SATURN
01200	.99.04-N4-00	01	OVER 5000 PSIG,SHUT,GLOBE,MANUAL	GROVE VALV	1113340-68	IPTU	04/67	SATURN
01100	.73.14-N4-01	01	100-1000 PSIG,SHUT,BALL,MANUAL	HILLS-MC	F402-S6-T	CDIPTU	12/67	SATURN
01102	.73.17-N4-01	01	100-1000 PSIG,SHUT,BALL,PRESS	HYDROPATIC	23157	CRILNPSTV	02/68	SATURN
01284	.95.04-N4-11	01	OVER 5000 PSIG,SHUT,MANUAL	J.PRO.CLAM	8R9-871-668 F9	CDIPTU	07/67	SATURN
00173	.73.47-N4-01	01	100-1000 PSIG,RELIEF,POP,PRESS	J.PRO.CLAM	8R9871-128-4	CRLPTU	0 /67	SATURN
00250	.03.47-N7-02	02	0-100 PSIG,RELIEF,POP,PRESS	J.PRO.CLAM	P-13-349	LTUV	12/63	SIGMUND
00254	.03.47-N7-01	01	0-100 PSIG,RELIEF,POP,PRESS	PROWLER	2163404 REV. M	LTUV	10/65	SIGMUND
01016	.65.07-N4-01	01	0-100 PSIG,RELIEF,PRESS	KENSIN V	600-F	ITTU	05/67	SATURN
00176	.05.47-N4-01	01	1350-5000 PSIG,RELIEF,POP,PRESS	KOMOTTA V	725844-301	CRLPTUV	04/66	SATURN
01019	.05.47-N4-C1	01	0-100 PSIG,RELIEF,POP,PRESS	MISSION V	1-3488	IPTU	04/67	SATURN
00437	.73.47-N4-C2	01	100-1000 PSIG,RELIEF,POP,PRESS	MISSION V	2-457	IUP	08/66	SATURN
01100	.99.47-N4-01	01	OVER 5000 PSIG,RELIEF,POP,PRESS	MISSION V	600-FF-11C	ITU	07/67	NASA
01102	.99.04-N4-00	01	OVER 5000 PSIG,SHUT,GLOBE,MANUAL	PAC VALVE	376-5-172504-12A-6A	CDIPTU	05/68	SATURN
01110	.75.17-N4-C2	01	100-1000 PSIG,SHUT,BALL,PRESS	PARKER A/C	F91-7	IPTT/UU	01/67	SATURN
00463	.73.47-P1-13	02	130-1000 PSIG,RELIEF,POP,PRESS	PARKER A/C	5671277	UUV	04/66	APOLLO
00466	.73.47-P1-13	01	130-1000 PSIG,RELIEF,POP,PRESS	PARKER A/C	5671235	LUV	04/68	APOLLO
01139	.A2.77-P1-05	01	1250-5000 PSIG,MAL7-FUNCT,SPOOL,PRE	ROYAL IND.	11327-PSCLASS I	IPU	06/68	APOLLO
01130	.82.77-P1-04	01	1650-5000 PSIG,MAL7-FUNCT,SPOOL,PRE	ROYAL IND.	11347-P3	IP	05/68	APOLLO
00260	.03.47-P1-04	01	1650-5000 PSIG,RELIEF,PRESS	ROYAL IND.	11327-2	UV	04/67	SATURN
00250	.03.47-N4-01	01	1350-5000 PSIG,RELIEF,POP,PRESS	SAGE ENGRG	1-5259	-----	05/66	SATURN
01101	.95.04-N4-01	01	OVER 5000 PSIG,MANUAL	SAGE ENGRG	1-5259C	CIPTU	04/67	SATURN
01141	.95.04-N4-01	01	OVER 5000 PSIG,MANUAL	SAGE ENGRG	1-5259D	CIPTU	04/67	SATURN
00178	.99.47-N4-03	01	OVER 5000 PSIG,RELIEF,POP,PRESS	SAGE ENGRG	501-16	IU	05/65	SATURN
00177	.93.47-N4-02	01	OVER 5000 PSIG,RELIEF,POP,PRESS	SAGE ENGRG	501-16	I	01/65	SATURN
01207	.01.44-P1-05	02	1000-5000 PSIG,CHECK,POP,MANUAL	SNAP TITE	2772-12	ITU	09/00	SATURN
01207	.01.44-P1-05	01	1000-5000 PSIG,CHECK,POP,MANUAL	SNAP TITE	2772-1	ITU	09/00	SATURN
00460	.99.04-N4-06	01	OVER 5000 PSIG,SHUT,MANUAL	VACCO VAL	M-10P-X4011-2G	IPTU	03/66	SATURN
00454	.99.04-N4-04	01	OVER 5000 PSIG,SHUT,MANUAL	VACCO VAL	M-10P-X4012-2G	IPTU	03/66	SATURN
00455	.99.04-N4-03	01	OVER 5000 PSIG,SHUT,MANUAL	VACCO VAL	M-10P-X401-2G	IPTU	08/65	SATURN
01207	.99.04-N4-12	01	OVER 5000 PSIG,SHUT,MANUAL	VACCO VAL	MA-6P-X403-2G	IP	05/68	SATURN
00465	.99.04-N4-02	01	OVER 5000 PSIG,SHUT,MANUAL	VACCO VAL	MVA-6P-401-2G	IPT/U	03/63	SATURN
00903	.99.04-N4-C1	01	OVER 5000 PSIG,SHUT,MANUAL	VACCO VAL	MVA-6P-402-2G	IPT/U	04/63	SATURN
01200	.99.04-N4-07	01	OVER 5000 PSIG,SHUT,GLOBE,MANUAL	VACCO VAL	M-6P-X403-2G	IP	05/68	SATURN
01103	.99.04-N4-09	01	OVER 5000 PSIG,SHUT,MANUAL	WORTHINGTON	MODEL 3611	IPTU	04/67	SATURN

Fig. 6 Extract from IDEP Index of Reports

Figure 7 illustrates how data is stored and retrieved at an IDEP office. The IDEP information storage and retrieval system is designed for rapid, error-free use without elaborate equipment. It enables an engineer to have easy access to the information desired within a few minutes. The microfilmed reports may be viewed or reproduced in easily readable size.

Currently there are over 30,000 reports on file, estimated to have cost at least $50 million to create. Each month approximately 250 new reports are added to the data bank.

Fig. 7 Portion of an IDEP Office Storage and Retrieval Center

FARADA

In contrast to IDEP which has three offices, there is only one FARADA Information Center, and that is located at FMSAEG, Corona, California. Participants in the FARADA Program submit information on field/fleet performance data on parts/components to the FARADA Information Center, where it is screened, analyzed, summarized, computerized, compiled, and disseminated, on a periodic basis, to all participants. The information is stored in loose leaf binder notebooks or handbooks, rather than on microfilm. The FARADA handbooks contain failure rates, generally expressed in terms of number of failures per million operating hours. Also contained therein is information pertaining to where the equipment was operated, what environmental conditions were experienced, modes of failure, and stress curves (for electrical and electronic parts/components).

The flow of data in the FARADA Program is shown in Figure 8.

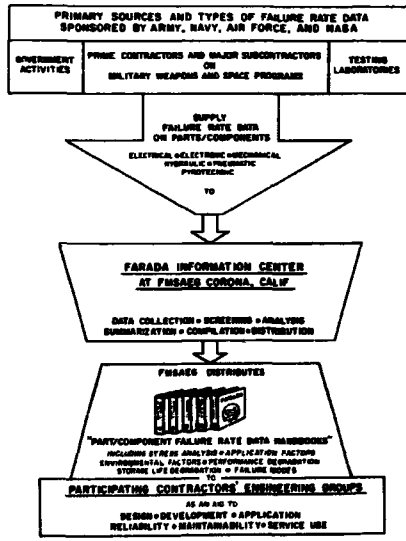


Fig. 8 FARADA Data Flow

Figures 9, 10, 11, 12, and 13 illustrate the handbooks and examples of the types of information pertaining to mechanical parts/components (contained in the handbooks) which are distributed to program participants. These handbooks presently contain approximately 45,000 line entries of tabulated failure rate data.

FARADA also provides an updating and expansion to the failure rate data appearing in MIL-HDBK-217, "Military Standardization Handbook," which is presently being revised to include failure rates for mechanical parts/components, as well as electrical/electronic parts/components. Both FARADA and MIL-HDBK-217 provide a basis for reliability prediction as outlined in MIL-STD-756A, "Reliability Prediction Procedures."

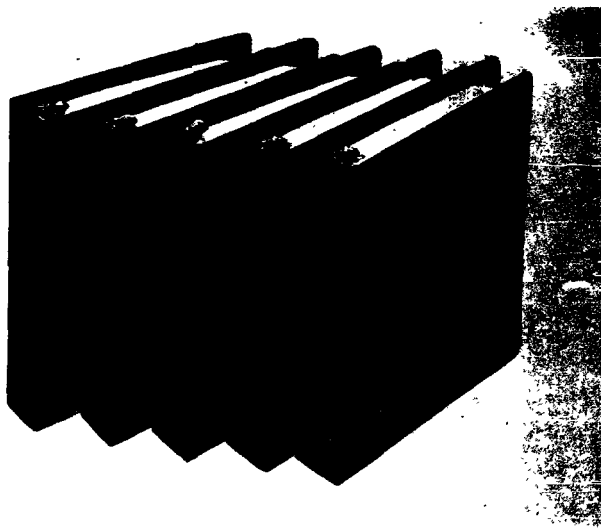


Fig. 9 Failure Rate Data Handbooks

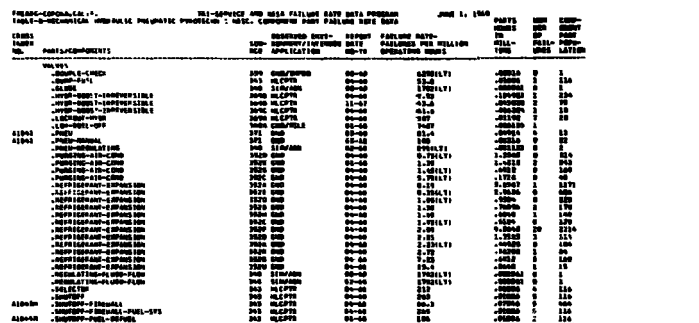


Fig. 10 Extract from FARADA Handbook Showing Failure Rates on Partial Listing of Valves

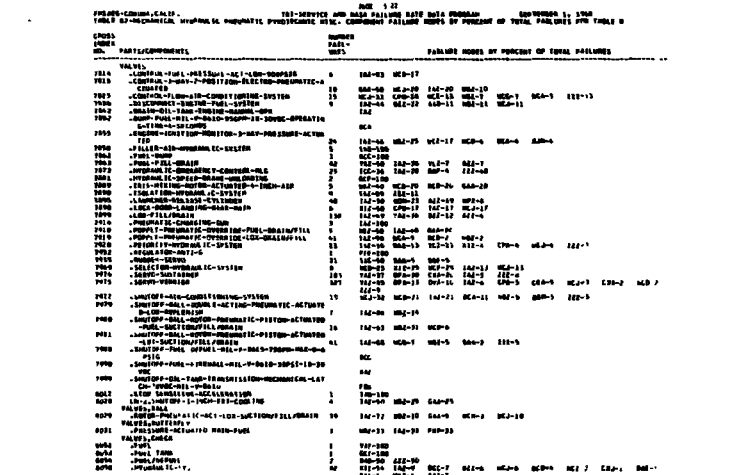
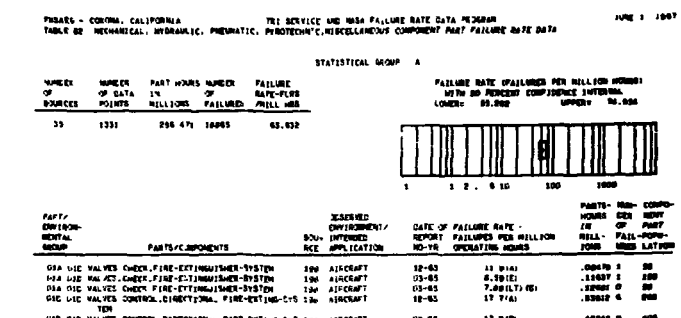


Fig. 11 Extract from FARADA Handbook Showing Modes of Failure for Partial Listing of Valves



FARADA - CORONA, CALIFORNIA TRI SERVICE AND NASA FAILURE RATE DATA PROGRAM JUNE 1 1967
TABLE 02 MECHANICAL, HYDRAULIC, PNEUMATIC, PYROTECHNIC, MISCELLANEOUS COMPONENT PART FAILURE RATE DATA

STATISTICAL GROUP A

NUMBER OF SOURCES	NUMBER OF DATA POINTS	PART HOURS IN MILLIONS	NUMBER OF FAILURES	FAILURE RATE /MILL HRS
39	1331	298.471	18465	63.032

FAILURE RATE (FAILURES PER MILLION HOURS)
WITH 90 PERCENT CONFIDENCE INTERVAL
LOWER= 59.988 UPPER= 66.266

1 1 2 . 5 10 100 1000

PART/ ENVIRON-MENTAL GROUP	PARTS/COMPONENTS	SOURCE	RESERVED ENVIRONMENT/ INTENDED APPLICATION	DATE OF REPORT NO-YR	FAILURE RATE - FAILURES PER MILLION OPERATING HOURS	PARTS-HOURS IN MILLIONS	NUMBER OF FAILURES	COMPONENT PART FAILURE RATE
01A 01C	VALVES CHECK,FIRE-EXTINGUISHER-SYSTEM	100	AIRCRAFT	12-63	13.9(A)	.006478	1	50
01A 02E	VALVES,CHECK,FIRE-EXTINGUISHER-SYSTEM	100	AIRCRAFT	03-65	8.59(E)	.116537	1	100
01A 01C	VALVES CHECK FIRE-EXTINGUISHER-SYSTEM	100	AIRCRAFT	03-65	7.69(LT) (E)	.129981	0	50
01C 01C	VALVES CONTROL,DIRECTIONAL FIRE-EXTING-SYS TEM	100	AIRCRAFT	12-65	17.7(A)	.05912	0	200
01E 01C	VALVES.CONTROL.DIRECTIONAL.FIRE-EXTING-SYS TEM	100	AIRCRAFT	03-65	17.2(E)	.05966	0	400
01E 01E	VALVES.CONTROL.DIRECTIONAL.FIRE-EXTING-SYS TEM	100	AIRCRAFT	03-65	104(E)	.00763	53	200
01B 01B	VALVES,DIRECTIONAL-FLOW,FIRE-EXT-SYS	297	AIRCRAFT	12-65	10.1(LT)	.09899	0	197
01D 01E	VALVES,DIRECTIONAL-FLOW,FIRE-EXT-SYS	200	AIRCRAFT	08-66	6.06(LT)	.1651	0	354
01C 01B	VALVES,DRAIN,FIRE-EXT-SYS	297	AIRCRAFT	12-65	20.2(LT)	.04944	0	66
01C 01B	VALVES,DRAIN,FIRE-EXT-SYS	200	AIRCRAFT	06-66	12.1(LT)	.08256	0	132
02 01	VALVES,DYPASS,HYDRAULIC-MANUAL	70	AIRCRAFT	01-59	36	.139	5	
02 01	VALVES,SOLENOID,HYDRAULIC	71	AIRCRAFT	01-59	434	.138	60	
02 01	VALVES,HYDRAULIC	71	AIRCRAFT	01-58	463	.130	94	
02 01A	VALVES,CONTROL,MANUAL,TIP-PROTECTION-GEAR	111	AIRCRAFT	02-63	126	.08187	3	50
02 01A	VALVES,BYPASS,GUN-TURRET,FIRE-CONTROL-SYST EM	111	AIRCRAFT	02-63	291	.03184	3	31
02 01A	VALVES,CONTROL,TEMPERATURE,OIL ENGINE	111	AIRCRAFT	02-63	15.5(LT)	.0035	8	848
02 01A	VALVES,HYDRAULIC AFTERBURNER-IGNITION	123	AIRCRAFT	07-63	326.75	.00538	33	
02 01A	VALVES,BYPASS,HYDRAULIC,STEERING,WHEEL-ACT.	170	AIRCRAFT	12-64	22.0	.00766	0	400

Fig. 12 Extract from FARADA Handbook Showing Converged Failure Rate Data (with 90% confidence intervals) on Partial Listing of Valves

PARTICIPATION REQUIREMENTS

Eligibility for participation in these data exchange programs is limited to Government agencies and contractors who are users of parts/components procured for incorporation into the design, development, or production of equipment for military and aerospace programs. Both IDEP and FARADA were established on a voluntary basis, and both continue to be voluntary programs, with no fees or assessments levied against the participants.

An important requirement stipulated to by IDEP participants is that a part/component manufacturer must be supplied a copy of any test report or results of a test performed on his product by the participant who performed the testing, prior to the report's being circularized within the program.

TABULAR FAILURE MODE DATA SUMMARY PARADA PROGRAM
TMD-PARADA-000 11 (REV. 1-68)

ACME COMPANY — 123 — 1 AUGUST 1969

"BACKGROUND INFORMATION ON FAILURE MODE DATA" should also be provided

PART COMPONENT COMPLETE NOMENCLATURE (Abbreviations including Mil. Spec. No. if applicable)	VENDOR AND VENDOR PART NO. MIL STD PART NO OR FEDERAL STOCK NUMBER	DESIGNATION ENVIRONMENT	INTENDED INSTALLATION ENVIRONMENT	FAILURE MODES AND NUMBER OF FAILURES: OVER HEATING	BINDING	JAMMING	MECHANICAL DAMAGE	PRESSURE FLUCTUATES	INDICATOR DEFECTIVE	CRACKED	LEAKING	OUT OF TOLERANCE	OPERATION ERRATIC	CHATTERING	OPERATION INTERMITTENT	FLUCTUATES	INOPERATIVE	OVERAL, AT IMPROPER	POSITIONING IMPROPER	CONTAMINATION	CORROSION
VALVE-CONTROL-FUEL-PRESSURE-ACT-LOK-900? SIC	NORTH AMERICAN AVIATION 9512-68A10-61	GROUND	MISSILE								5		1								
VALVE-CONTROL-3-WAY-2-POSITION-ELECTRO-PNEUMATIC-ACTUATED	MAROTTA VALVE 2-70164	GROUND	MISSILE						5		2	1					2				
VALVE-CONTROL-FLOW-AIR-CONDITIONING-SYSTEM	HYDRAULIC RESEARCH 11-1000	AIRCRAFT	AIRCRAFT		1			3				1		1		2	3				
VALVE-DISCONNECT-ENGINE-FUEL-SYSTEM	HYDRAULIC RESEARCH 11-1200	HELICOPTER	HELICOPTER	1			2			1	4						1				
VALVE-DRAIN-OIL-TANK-ENGINE-MANUAL-OPR	SPARTAN HYDRAULICS 702-12	HELICOPTER	HELICOPTER			4					2										
VALVE-DROP-FUEL-MIL-V-8610-93GEN-18-30SEC-OPERATING-TIME-4-SECONDS	ADEL PRECISION PRODUCTS 29953-4	HELICOPTER	HELICOPTER			6								3					1		
VALVE-IGNITER-IGNITION-MONITOR-3-WAY-PNEUMATIC-ACTUATED	ADEL PRECISION PRODUCTS 216/3-10	GROUND	MISSILE		1						11	6			1			4	1		
VALVE-FILLED-AIR-HYDRAULIC-SYSTEM	W.OEHLER 106023-32	AIRCRAFT	AIRCRAFT								3										
VALVE-FUEL-DUMP	BENTON CORP. 110673	AIRCRAFT	AIRCRAFT			1															
VALVE-FUEL-FILLER-MAIN	OEHLER 103064-552	GROUND	MISSILE				3				15									21	3

Fig. 13 Tabular Failure Mode Data Summary - PARADA Program

SUMMARY

Through the media of these data exchange programs, IDEP and FARADA, the design engineer and the reliability/maintainability/safety engineer have two powerful tools at their disposal. The proper utilization of data--as a commodity--has a tremendous impact on the reliability/maintainability, safety, and performance of a missile or an aerospace system. A basic precept of the programs is that the information is waiting for the engineer rather than vice versa.

These data exchange programs have benefitted Government, Industry, and Taxpayers through a reduction in hardware development costs exceeding many millions of dollars each year. A recent IDEP survey documented over $5 million in savings attributed to the reduction of testing and the consequent elimination of test hardware purchases. The time, money, and effort saved was directed instead toward improving the reliability/maintainability of the product.

The requirement that IDEP participants provide a part/component manufacturer with results of tests performed on his product before the report is circularized within the program has, in no small measure, helped to create more reliable parts/components.

Other benefits and objectives of these data exchange programs are

- Realistic bid proposals through access to current parts information.
- Reliable parts selection in designs to avoid possible systems failures.
- Advance parts information to promote improved performance.
- Shortened delivery schedules.
- Improved test reporting with resultant higher output per test dollar.
- Accelerated parts specification writing and test planning--expediting introduction of standard improved parts.
- Provision for direct intercontractor inquiries in urgent cases.
- Suggested alternate vendor sources.
- Source of general advice, confirmation, and general education in early stages of program development.

The IDEP and FARADA data exchange programs represent an outstanding example of cooperation and team work between Government and Industry; without these ingredients, achievement of program objectives could not have been successful.

Further information may be obtained by writing to

Commanding Officer
Naval Fleet Missile Systems
Analysis and Evaluation Group
Corona, California 91720.

N E S A - I F V
Research Department
jeh.vbr

19th September, 1969
R 1969-78

Paper No. 20

AVAILABILITY AND FAULT ANALYSIS OF THERMAL GENERATING EQUIPMENT

by
J. Ehlert Knudsen
Nordsjællands Elektricitets- og
Sporvejs Aktieselskab. Hellerup

---oOo---

OECD - ENEA Meeting of
Specialists on the Reliability of Mechanical
Components and Systems for Nuclear Reactor Safety
Risø, 24th - 26th September, 1969

---oOo---

Introduction

The pursuit of an ever increasing efficiency and of improved construction and operation economy has in the past been very successful as demonstrated by the decreased power plant heat-rates and reductions in specific costs and in operating expenses.

These improvements have been obtained partly due to higher temperatures, pressures, reheat-cycles, etc. and partly due to increased unit sizes. Inevitably the plant has become more complicated - and thus more vulnerable to disturbances. Improvements in economy and installation costs have to some extent been paid by a reduction of the operational reliability, especially during the first few years of operation of not yet matured types.

This has caused considerable concern in power companies all over the world and has turned the attention towards more detailed studies of plant availability and reliability. So far the choice of construction deemed necessary has been based largely upon personal

experiences and discussions as well as exchange of information nationally and internationally with colleagues having similar experiences. It has now been realized that the decisions to be made can be supported by objective statistical information collected on a nation-wide basis in a uniform way and treated identically so that the results can be exchanged and reliable comparisons be made.

The statistical information should cover a reasonable number of years and the greatest number of units possible with a minimum of time between the recordings of performance and the analysis of the information. Bearing in mind that the emphasis placed upon the restoring of equipment to normal operational status after a failure largely affects the reliability figures - expressed as outage rates - some means of characterizing this emphasis should be devised.

The results should not only allow an evaluation of past and present operating experiences, thereby determining the principal causes of unavailability, but should also allow a projection for future installations by the provision of a sound basis for engineering studies leading to corrections of the weak points.

Statistical information about the behaviour of overhead lines and electrical apparatus has been collected over a very long period of years, and results are regularly published. A comparison between different systems and a recognition of defects have been possible through these statistics. It is generally accepted that such statistical information is valuable for system planning and operation with a view to the optimal economic result.

Similar view-points ought to be applied more widely on power plant components, where the objective of design and operation engineers is the same: to aim at the highest possible reliability compatible with sound economics.

Availability statistics are collected in every power company - but in many various ways. Much effort is laid down in attempts to uniform the methods of collection and of treatment of the data, and as a first step an agreement about the fundamental definitions must be obtained. The work carried out in the United States of the Edison Electric Institute, Prime Movers Committee (its Equipment Availabi-

lity Task Force) and the IEEE Joint Subcommittee on Application of Probability Methods has been fundamental in this respect. In Europe the definitions adopted by UNIPEDE have been limited, mainly with a view to the application in determining necessary installed power. Analysis of and comparisons between various definitions and measures of availability have been presented in a number of publications, and recently the Economic Commission of Europe has compared the definitions in the papers EP/WP.6/Working Paper No. 42 and EP/WP.4/Working Paper No. 19.

Whichever method is used to gather information about availability, it is normal practice to indicate the availabilities for different categories of power plant: low pressure; high pressure without reheat; high pressure with reheat and various unit sizes; etc. Furthermore the main components: boiler; turbine; condenser; generator; etc. are treated separately, and in some cases a limited number of auxiliary equipment as: cyclones; pulverizers; induced draft fans; forced draft fans; condensate pumps; condenser circulating water pumps; exciters; boiler feed pumps; etc. are studied in detail in order to permit a separate analysis of their operational performance.

The evaluation of the reliability of various components, as it can be deduced as by-products of availability studies, suffers generally from one important drawback: only such incidents that affect the capability of the unit are recorded.

Repairs, which are carried out without affecting the capability - e.g. repair of a reserve feed-water pump, while the other suffice to secure full load - or repairs carried out during a breakdown of another component are not normally reported, as they do not influence the availability of the unit as such.

Some notes are, however, normally made in the power stations in connection with repairs of equipment, but very often these notes are made in a more of less casual way and without any systematic organization. This makes special studies of particular components practically impossible.

A systematic recording of all repairs, whether they influence the

capability or not, has been introduced in Germany by RWE *). A similar procedure is on trial in France and is also under discussion in Great Britain and in the NORDEL-countries. The problem is to find the golden mean between the easy simplification and the perfection that might impose too much extra work on the power station operators.

Collection of Statistical Information

In the United States the main source of information about outages has been the data collected by the Edison Electric Institute, Prime Movers Committee, since 1938. Results covering a number of years are regularly published. - The latest publication (EEI No. 68-24) issued August 1968 covers the eight-year period 1960-67.

In cooperation with the IEEE Joint Subcommittee on Application of Probability Methods a Manual for Reporting the Performance of Generating Equipment has been made effective from 1st January, 1968. The reporting form is filled in by the operator on duty who uses special code tables to indicate operating data, outage causes, information about manufacture, etc. Data giving information about changes taking place in the operation (outages or deratings) are filled in simultaneously with the events.

The aims of the reporting have been to make only one recording, demanding only a minimum of time - and in a form suitable for digital computer treatment. The recorded data should be sufficiently detailed to allow for other applications than just outage rates for the main components in different categories of plant.

In Europe the member-countries of UNIPEDE (International Union of Producers and Distributors of Electricity) have formed a working group under the Statistics Study Committee to deal with the problem of availability of thermal power plant.

It has been agreed to collect and exchange information about available power giving monthly figures that are based upon the power

*) Verfügbarkeits- und Schadensstatistik als Entscheidungshilfe für Bau und Betrieb von Kraftwerken.

H. Vetter and K. Neuroth, Mitt. der VGB, 48 Heft 2, April 1968.

available each day at eight a.m. (not including Saturdays, Sundays, and holidays). Unavailability is divided between planned maintenance and all other causes. Information is collected separately for thermal units 100-199 MW and 200-400 MW.

Although a considerable amount of data have been collected from about 10 countries no figures have so far been published. A number of studies have tried to reveal tendencies in the availability with age or size of the units. Furthermore some analysis of the availability of the main components has been carried out and more is in progress.

Within the NORDEL-countries a systematic reporting procedure for thermal power plant availability was started in Denmark - as the pure thermal power country in Scandinavia - already in 1957. From the beginning of the sixties a standardized reporting procedure was tested and in January 1964 adopted nationally by all Danish power companies. The reporting procedure is very much similar to the US practice.

Simultaneous efforts in Sweden led to a close cooperation manifested within the NORDEL organization, in which also Finland has later expressed great interest in thermal power availability. Small working groups within each of the three countries conduct the statistical work and cooperate within the NORDEL working group.

The reporting forms used in the Scandinavian countries have only minor deviations, and the results are published by NORDEL - together with other statistics on the operational performance of equipment as lines transformers etc.

Even if results from all NORDEL-countries are included, the breadth of these is very limited. Consequently it is important to include results from other countries (especially when the operational reliability of future large units is estimated). Great efforts are made by NORDEL to intensify the international cooperation in this field and to make exchange of information more open-minded. In order that the results are comparable it is naturally necessary that the statistical data are bases on comparable standards. The NORDEL statistics are therefore made sufficinetly flexible to enable comparison with

US results as well as results from the cooperating countries within UNIPEDE.

Definitions of the Factors Characterizing Availability

Two different approaches with respect to defining numerical figures are at present in use. In the US (as well as in NORDEL) time is used as the basis for determining availability and forced outage rates.

On this basis the availability factor is defined as the ratio of the time in which the plant has been available (it be in operation or in reserve) to the total time. The tall, shaded columns in fig. 1 show the results obtained for all Danish power stations 1964-1968 and separately given for units, boilers, and turbo-generators. The tapes show the accumulated values since 1964. The forced outage rate is defined as the ratio of total outage time to the sum of total outage time and total operation time. In fig. 1 the results in Denmark are shown as the lower (unshaded) columns. Numerical figures corresponding to fig. 1 are given in table 1.

One difficulty in using time as the basis arised when outages are only partial, in other words when deratings from full nominal power are to be taken into consideration. Normally such deratings are included as equivalent full forced outages having a reduced outage time proportional to the relative amount of the derating.

While the available time or time on forced outage are normally easy to determine, the question is often raised about scheduled outages that is such outages which have not been planned at the time when the maintenance programm is fixed, but which can be planned some time in advance or for which the starting date is controllable beyond the week-end of the week in which some component trouble occurred.

In the UNIPEDE statistics such scheduled outages are considered as unavailability due to other causes than planned maintenance. They thus contribute to increase the unavailability factor.

In UNIPEDE power has been chosen as the basis for determining availability factors, taking as a measure of available power the morning peak during which the load dispatcher has a knowledge of what is

actually at his disposal for the day. The availability factor, e.g. for a month is calculated by dividing the product-sum of available power each working day by the total energy producible if all installed power were available each working day.

Fig. 2 illustrates the results thus obtained for Danish units between 100 and 199 MW. The black columns include planned maintenance, and the white sections of the columns indicate how much the maintenance has contributed to reduce the availability. The annual averages are indicated in the figure.

Fig. 3 gives an example of a graph - often used in UNIPEDE - showing the relative length of time during which the available power is larger than or equal to the percentage indicated on the abscissa. Very often such graphs will disclose the fact that the total installed power has never been available at any time - due to maintenance or to outages.

In fig. 4 is shown a distribution function of forced outage power showing the ratio of power forced out to total power plotted in decreasing order. The curve is based upon the situation each working day at 8.00. The dashed curves have been drawn as the curves resulting from probability calculations assuming 7 % or 5 % forced outage rate. By comparison between the theoretical 5 % curve and the empirically determined full curve it seems like a 5 % forced outage rate is a reasonable assumption in the particular case.

Analysis of Results

Experiences outside Scandinavia have indicated that especially during the first years after commissioning, the new large units have significantly higher outage rates and lower availability than smaller proven units. This is illustrated by fig. 5 (taken from EEI publ. 68-24) and is also confirmed by the unpublished figures collected in UNIPEDE. Examples of an analysis according to age is given in table 2 which seem to indicate a trend towards bad availability and forced outage rates for the oldest plant. There are, however, no significant teething-troubles for the (limited) amount of units included in the table.

The figures given in table 3 illustrate how an analysis according to size can be performed, and in table 4 is shown an analysis according to the number of operational hours per year. This clearly indicates a better availability of the plant having a higher operational time.

An attempt to disclose the maturing of units is made in table 5 arranging the availability factors for Danish units 100-199 MW according to age. The mean values - and especially the cumulated mean values at the columns to the right show a rather quick maturing effect.

Component Failure Analysis

While availability and forced outage statistics are of main concern for system planning engineers who have to determine the future amount of installed capacity - including necessary reserves - an analysis of component failures is of concern to the design and operation engineers.

An analysis of this kind is of the utmost importance in order to find the potential sources of failure leading to technical improvements or to a better understanding of the reserve requirements concerning for instance fans, feed pumps, control equipment, etc.

A number of reasons for establishing component failure statistics can be given:

1) An objective measure of each major component's responsibility for the overall availability should be given. Weak points can thus be found and characterized quantitatively. This must be basic to all efforts undertaken to improve the overall availability.

2) The determination of necessary reserve equipment is normally a matter of judgement. The total reliability of a unit is a function of the different component reliabilities, and when these are reasonably well known, reserves should be installed to such an extent that an optimum of availability is achieved. Quantitative information about the average unavailability factors, average duration of outages or mean time between outages of major components such as feed pumps, fans, turbine blades, generator rotors, etc. may give valuable guidance in the choice of reserve

equipment deemed necessary.

3) The extent, to which annual overhauls are carried out, varies greatly from one company to another. Damage statistics from companies having different overhaul practice may by comparison between the results lead to changes in policy.

4) Restricted to a national level - as an international exchange of information is entirely impossible within official channels - a direct comparison of component behaviour for various types or manufactures is desirable. This is not only true for the power companies that order the components, but also for the manufacturers, whose aim is to deliver reliable components, and whose research and development work must depend upon the operational experiences.

It has been found useful by everyone involved in this kind of statistics to develop some kind of outage code - in general a two or three digit code characterizing the components.

When treating the collected data in a computer, printouts of the number of faults and their duration for a given main group - first digit - (e.g. boiler) or subgroup - second digit - (e.g. economizer) can be produced for the total amount of equipment in the country or for any specified station. Further analysis with respect to age or to manufacturer can be included. An example of a printout for a particular unit listing all faults during a 4-year period in descending order of fault duration is given below:

Faulted part or symptom	Code	Hours	Hours in % of total	Number of faults
Furnace room evaporator tubes	113	226.2	19.8	9
Vibrations	319	216.3	18.9	48
Preheater flanges	402	145.3	12.7	1
Induced draft fan	242	107.8	9.4	10
Condenser tubes	362	107.0	9.4	34
HP wall superheater	122	92.6	8.1	3
HP radiation superheater	121	47.8	4.2	2
Feed water and condensate valves	473	42.4	3.7	2
Steam valves or tubes	470	38.7	3.4	2
Valves for compressed air or underblast	240	28.0	2.5	5
Preheaters feedwater pumps or tubes	499	18.2	1.6	1
Feed water valve or tube	173	17.7	1.5	1
Not spec. part in security system	349	11.9	1.0	2
Undefined cause in turbine	359	10.3	0.9	1
HP safety governor	331	9.0	0.8	1
Cooling water screen	372	8.2	0.7	1
Safety regulator	347	7.2	0.6	1
MP pick up valve	336	4.6	0.4	1
Undefined cause in feed pump	439	1.1	0.1	1
Primary electricity supply system	626	1.1	0.1	1
Other external causes	939	0.5	0.0	1
	Sum	1142.1	100.0	128

Graphically a similar analysis of main components causing outages or deratings in Danish power stations over a three-year period is shown in fig. 6.

Within UNIPEDE a simple code list indicating the main components has been applied to allow the (confidential) exchange of information about the number of outages, their duration, and the energy lost expressed in per thousands of the possible energy production. Only outages which cause reductions in power are, however, included so far. The tendency is to accept some extra burden upon the power station operators to obtain complete records of the performance of the main components in a power station - independant of their influence upon power output.

Further analysis, which yet has to be introduced, concerns a possible correlation between preventive maintenance and forced outage rates. By carrying out the preventive maintenance, some of the unit-availability is sacrificed - at a time when it can best be spared - in the

hope that the unit then stands a better chance of being available, when it is needed most.

As the problem of finding proper periods for preventive maintenance is becoming more and more difficult in pure thermal power systems having many large, highly efficient units, the repair effort - its cost and the labour required - should be carefully analyzed.

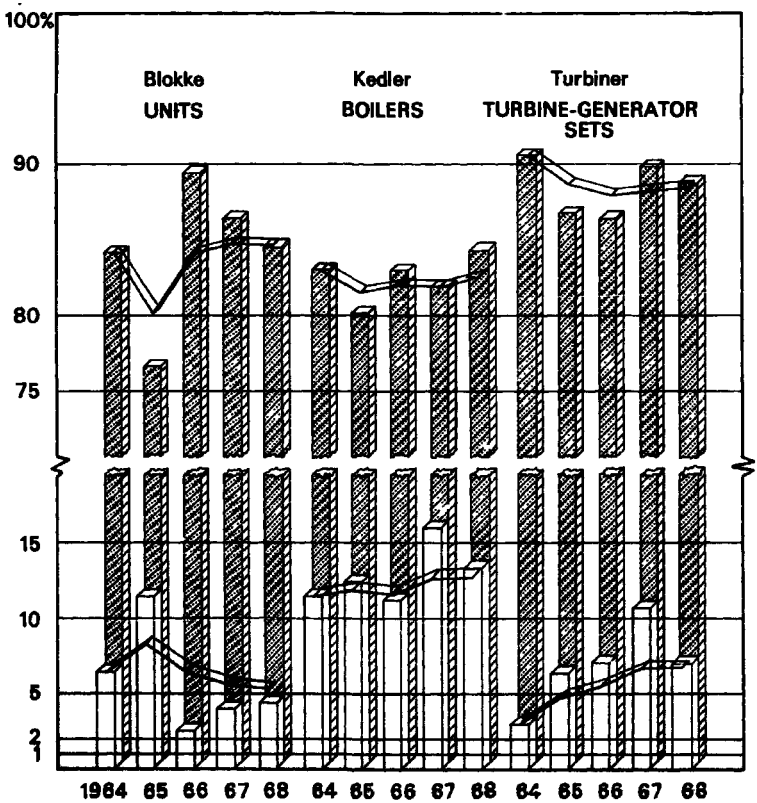
Conclusion

Exchange of information about availability and forced outage rates is undoubtedly of great value in system planning - provided that the figures are based upon uniform definitions. A more free publication of results obtained should be encouraged.

Fault analysis may not always be similarly interesting from one country to another, because design and manufacture vary greatly. Nevertheless information about methods used and general trends discovered should be published regularly, preferably by some international organization.

FIG.1

Havari- og rådighedstal for samtlige danske kraftværker



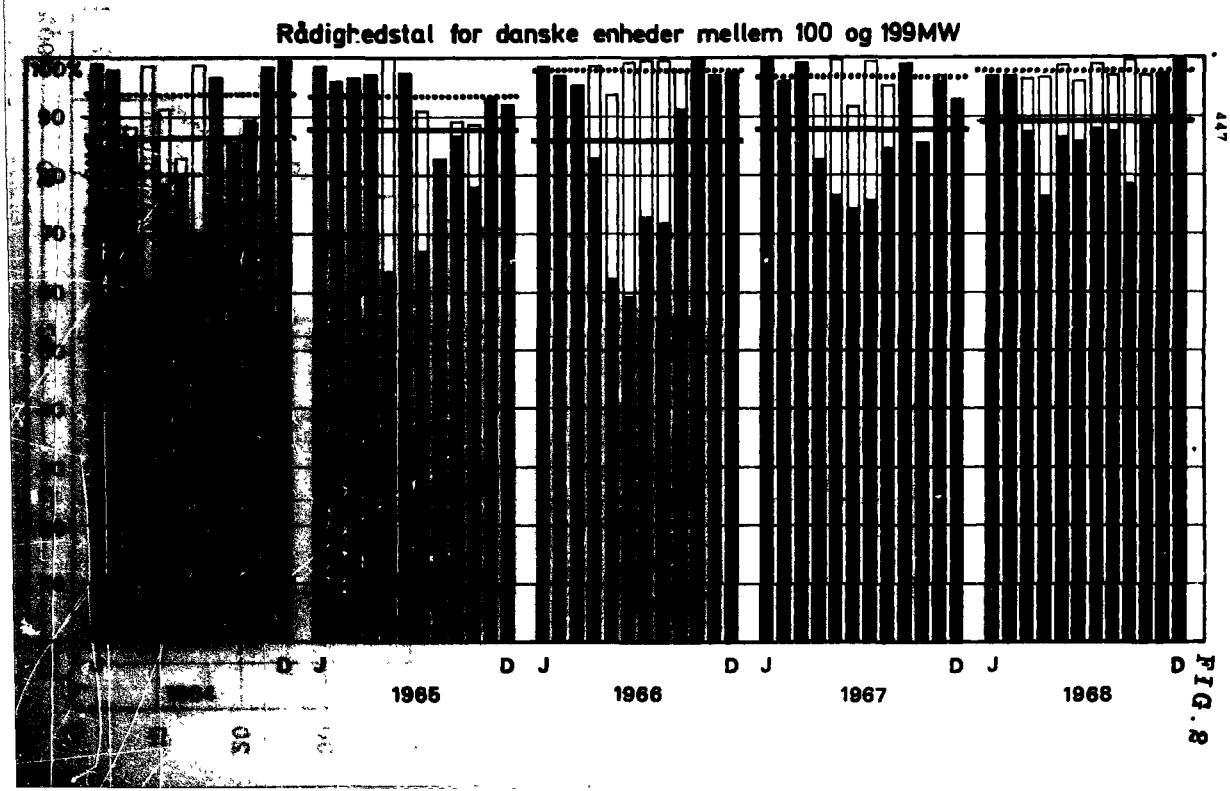

Rådighedstal for danske enheder mellem 100 og 199MW
100%
90
80
70
60
50
40
30
20
10
0
D
J
D
J
D
J
D
J
1965
1966
1967
1968
447

FIG. 8

FIG. 3

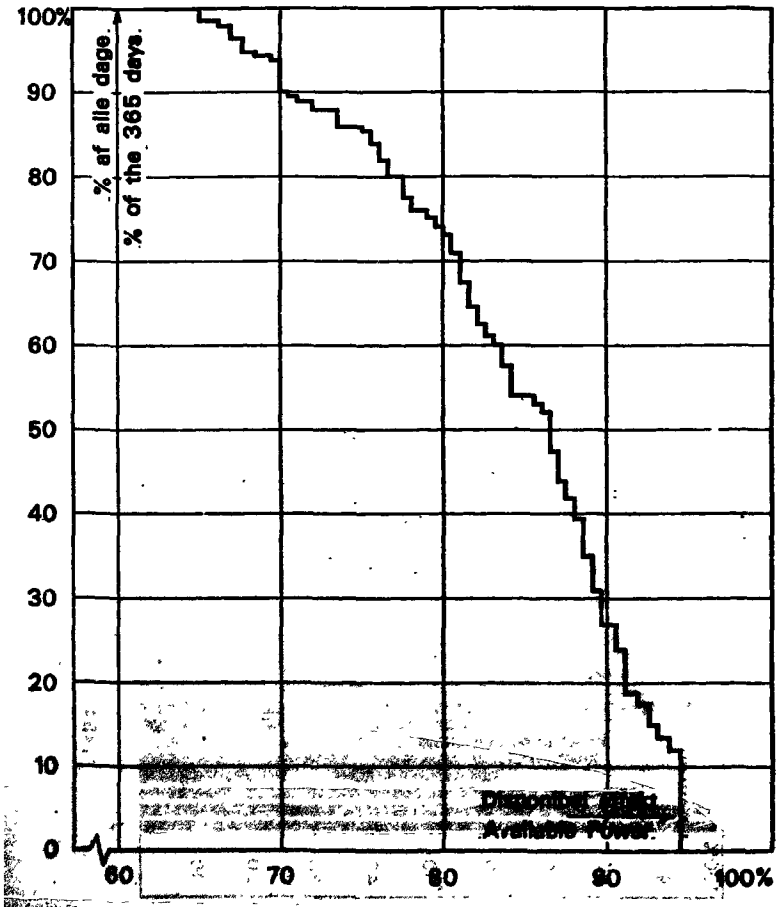
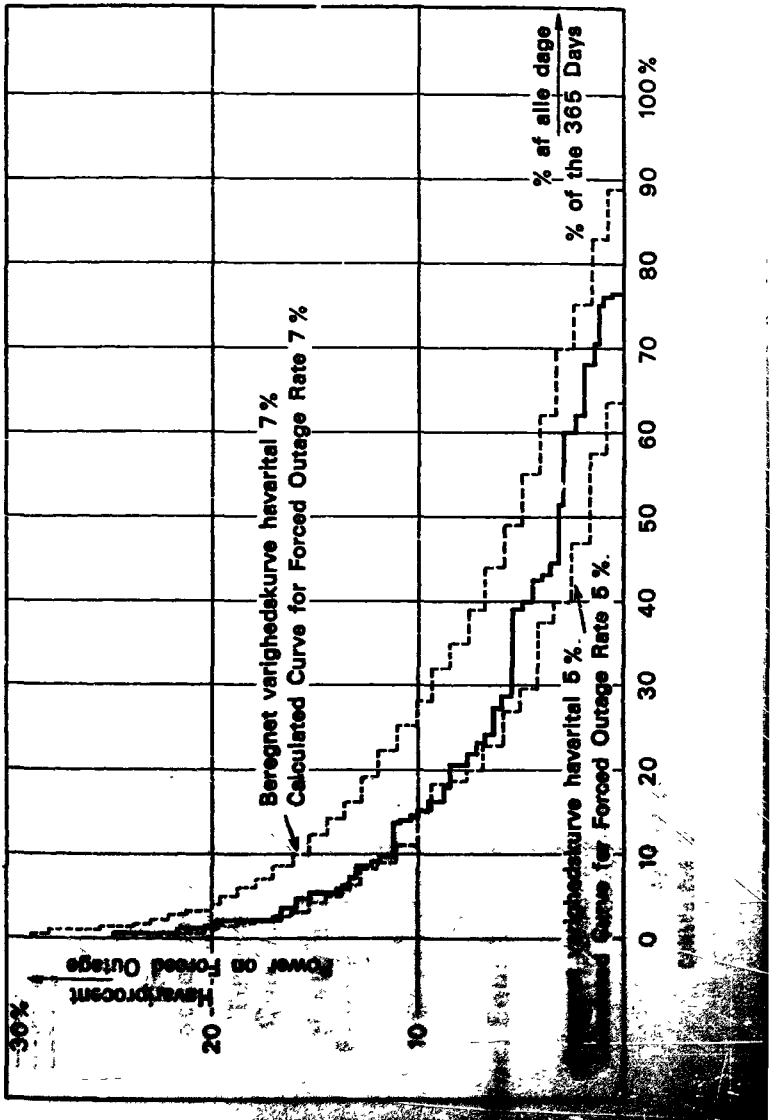

100%
90
80
70
60
50
40
30
20
10
0
% af alle dage.
% of the 365 days.
60
70
80
90
100%
Disponibel effekt.
Available Power.

FIG. 4


30%
20
10
Power on Forced Outage
Beregnet varighedskurve havarital 7 %
Calculated Curve for Forced Outage Rate 7 %
Varighedskurve havarital 5 %
Curve for Forced Outage Rate 5 %
0
10
20
30
40
50
60
70
80
90
100 %
% af alle dage
% of the 365 Days

IV MATURITY TRENDS

COMPARISON OF OPERATING AVAILABILITY, FORCED OUTAGE RATES AND SCHEDULED OUTAGE RATES VS YEAR OF OPERATION FOR DRUM-TYPE, ONCE-THROUGH, AND NUCLEAR UNITS

WEIGHTED AVERAGES

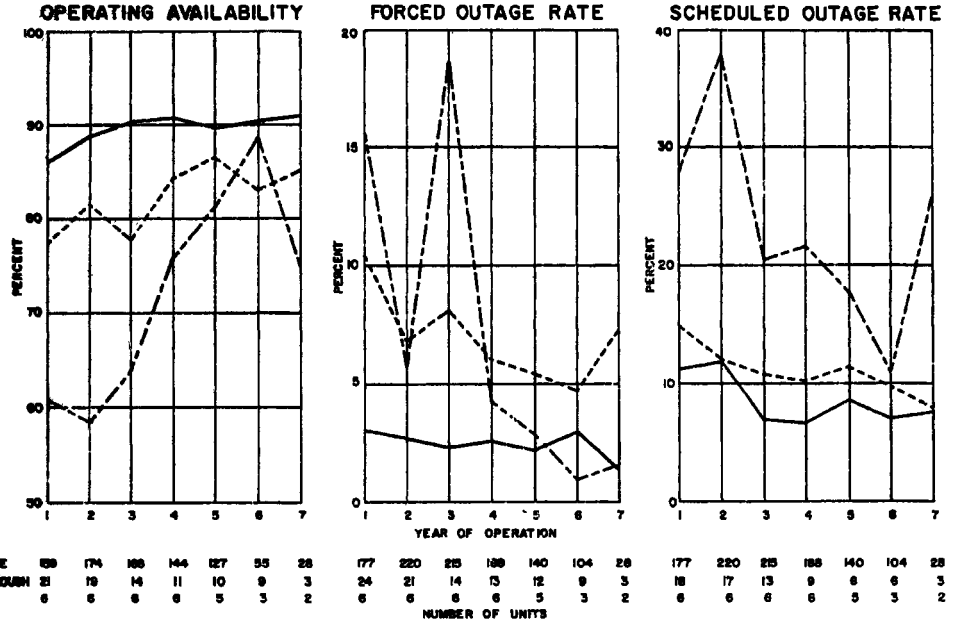


FIG. 5

FIG. 6

Fault analysis of all Danish power stations for the 3-years period 1966 – 1968.

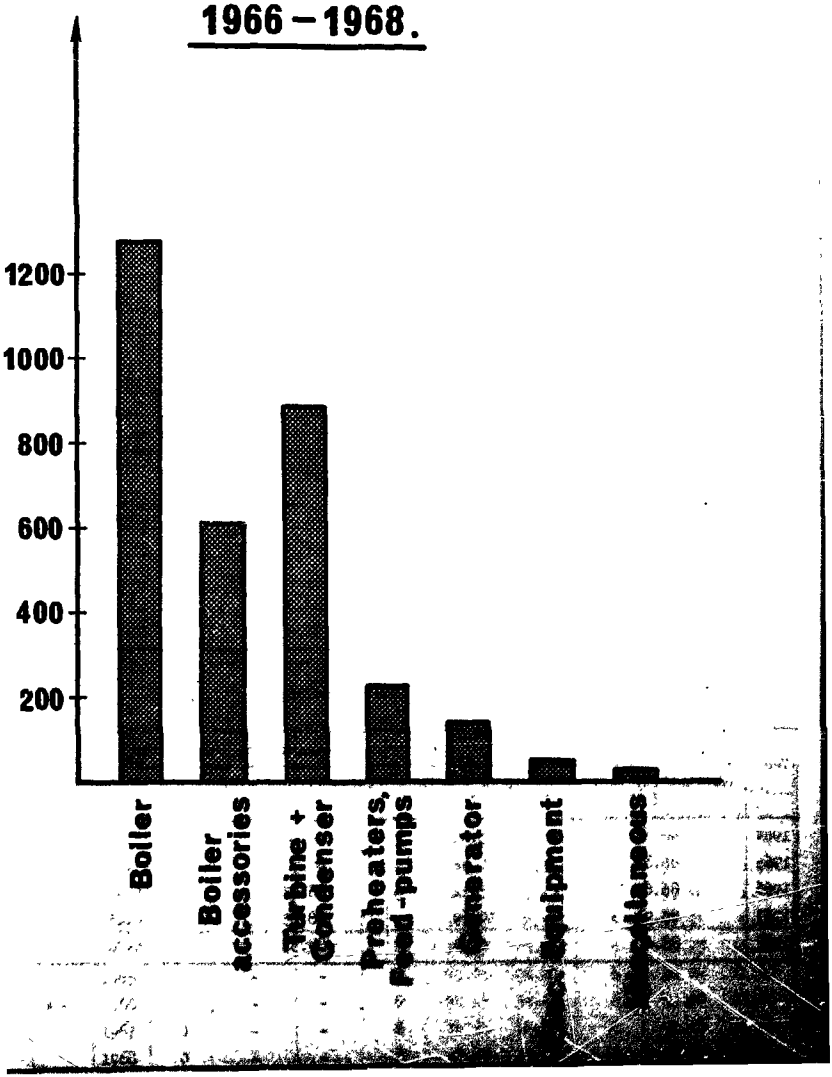


TABLE 1

Availability Factors and Forced Outage Rates for Danish Power Stations

Units

Year	Specific Year		Accumulated Values from 1964	
	Availability Factor %	Forced Outage Rate %	Availability Factor %	Forced Outage Rate %
1964	84.22	6.47	84.22	6.47
1965	76.75	11.58	80.12	9.23
1966	89.40	2.50	83.93	6.46
1967	86.44	4.05	84.80	5.64
1968	84.42	4.41	84.69	5.29

Boilers

Year	Specific Year		Accumulated Values from 1964	
	Availability Factor %	Forced Outage Rate %	Availability Factor %	Forced Outage Rate %
1964	83.04	11.43	83.04	11.43
1965	80.22	12.37	81.64	11.89
1966	83.02	11.19	82.08	11.65
1967	82.08	15.97	82.08	12.64
1968	84.24	13.21	82.50	12.74

Turbines and Generators

Year	Specific Year		Accumulated Values from 1964	
	Availability Factor %	Forced Outage Rate %	Availability Factor %	Forced Outage Rate %
1964	90.68	3.01	90.68	3.01
1965	86.81	6.42	88.73	4.70
1966	86.60	7.11	88.03	5.44
1967	88.94	10.69	88.25	6.65
1968	88.60	6.94	88.33	6.70

TABLE 2

Availability Factors and Forced Outage Rates for Danish Power Stations
The Plants Are Sorted According to Age

Age	Year	Units			Boilers			Turbines and Generators		
		Number of Units	Availability Factor %	Forced Outage Rate %	Number of Units	Availability Factor %	Forced Outage Rate %	Number of Units	Availability Factor %	Forced Outage Rate %
0-4	1964	4	83.99	7.18	8	75.72	12.69	3	85.70	2.92
	1965	5	85.04	6.69	7	84.02	8.20	4	86.19	11.36
	1966	3	83.93	3.87	7	81.61	9.12	4	91.72	7.31
	1967	5	87.74	4.22	7	76.86	18.00	2	86.41	5.86
	1968	9	85.95	5.58	3	86.70	5.11	2	83.94	15.98
5-9	1964	1	85.11	3.67	12	85.12	7.12	7	90.03	2.31
	1965	2	60.50	22.72	11	73.34	7.24	6	79.59	16.14
	1966	5	93.05	1.61	10	80.46	8.67	6	85.89	4.39
	1967	5	85.20	3.87	9	78.27	14.75	8	91.17	5.68
	1968	4	78.63	2.35	9	79.64	8.47	4	86.93	2.41
10-14	1964	0	-	-	26	85.08	7.83	17	89.24	1.56
	1965	0	-	-	27	79.52	9.23	19	84.04	2.81
	1966	0	-	-	24	83.34	6.53	16	86.43	3.11
	1967	0	-	-	22	81.50	9.36	15	88.10	7.51
	1968	1	97.20	3.09	13	83.20	13.81	11	87.67	0.82
15-19	1964	0	-	-	4	89.90	8.60	6	93.39	3.22
	1965	0	-	-	5	93.45	3.03	7	87.43	3.61
	1966	0	-	-	10	86.23	18.10	10	76.94	23.80
	1967	0	-	-	12	88.99	14.22	10	82.30	28.76
	1968	0	-	-	25	87.65	9.52	16	86.75	10.90
20-24	1964	0	-	-	6	86.69	15.33	5	95.09	2.27
	1965	0	-	-	1	79.78	1.83	1	80.81	1.88
	1966	0	-	-	1	83.37	3.24	0	-	-
	1967	0	-	-	0	-	-	0	-	-
	1968	0	-	-	0	-	-	2	90.62	26.55
25-29	1964	0	-	-	0	-	-	2	99.96	0.15
	1965	0	-	-	5	89.15	14.04	5	95.76	2.67
	1966	0	-	-	5	86.22	25.84	6	98.69	2.74
	1967	0	-	-	6	92.07	14.52	5	95.99	1.45
	1968	0	-	-	6	87.82	12.47	5	91.88	8.37
30-	1964	0	-	-	8	77.25	25.71	6	90.88	13.[illegible]
	1965	0	-	-	8	79.65	28.[illegible]	6	[illegible]	[illegible]
	1966	0	-	-	8	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	1967	0	-	-	8	73.[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	1968	0	-	-	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

TABLE 3

Availability Factor and Forced Outage Rate for Danish Power Stations
The Plants Are Sorted According to Size

Units
20-99 MW

Year	Number	Availability Factor %	Forced Outage Rate %
1964	2	82.83	6.18
1965	2	56.46	25.01
1966	3	96.38	2.42
1967	3	83.74	5.44
1968	3	78.01	3.83

Boilers
20-99 MW

Year	Number	Availability Factor %	Forced Outage Rate %
1964	41	83.24	9.09
1965	41	78.64	8.21
1966	41	82.28	8.56
1967	41	80.88	13.18
1968	41	83.61	9.66

100-199 MW

Year	Number	Availability Factor %	Forced Outage Rate %
1964	3	85.19	6.66
1965	5	87.11	6.01
1966	5	85.91	2.55
1967	7	87.64	3.56
1968	8	89.76	2.12

Turbines and Generators
20-99 MW

Year	Number	Availability Factor %	Forced Outage Rate %
1964	37	89.89	2.50
1965	39	85.28	7.06
1966	39	85.06	7.52
1967	37	87.14	10.99
1968	37	86.51	7.42

200-499 MW

Year	Number	Availability Factor %	Forced Outage Rate %
1968	3	71.62	16.87

TABLE 4

Availability Factor and Forced Outage Rate for Danish Power Stations

The Plants Are Sorted According to Operational Hours/Year

Units

Operational Time 1000-3999 Hours/Year

Year	Number	Availability Factor %	Forced Outage Rate %
1964	0	-	-
1965	1	29.13	54.75
1966	0	-	-
1967	0	-	-
1968	1	32.41	68.96

Operational Time ≥ 4000 Hours/Year

Year	Number	Availability Factor %	Forced Outage Rate %
1964	5	84.22	6.47
1965	6	86.43	5.38
1966	8	89.40	2.50
1967	10	86.44	4.05
1968	13	85.51	2.82

Boilers

0-999 Hours/Year

Year	Number	Availability Factor %	Forced Outage Rate %
1964	6	78.58	38.55
1965	2	88.51	60.26
1966	11	83.16	39.01
1967	9	82.97	60.24
1968	19	83.08	42.57

Turbines and Generators

0-999 Hours/Year

Year	Number	Availability Factor %	Forced Outage Rate %
1964	6	97.44	34.89
1965	6	95.50	7.07
1966	10	77.91	56.77
1967	7	96.11	41.72
1968	8	94.21	21.19

1000-3999 Hours/Year

Year	Number	Availability Factor %	Forced Outage Rate %
1964	31	83.28	18.50
1965	37	77.47	21.00
1966	32	84.02	16.41
1967	30	82.55	19.44
1968	18	86.84	19.59

1000-3999 Hours/Year

Year	Number	Availability Factor %	Forced Outage Rate %
1964	16	90.26	4.17
1965	20	83.83	10.83
1966	17	86.38	12.64
1967	18	89.37	20.92
1968	16	86.78	10.77

Operational Time ≥ 4000 Hours/Year

Year	Number	Availability Factor %	Forced Outage Rate %
1964	32	85.66	6.97
1965	30	82.97	6.60
1966	26	81.86	6.28
1967	25	81.19	10.21
1968	27	83.33	7.45

Operational Time ≥ 4000 Hours/Year

Year	Number	Availability Factor %	Forced Outage Rate %
1964	27	84.89	5.77
1965	27	87.48	4.38
1966	24	90.85	2.50
1967	22	88.29	3.97
1968	28	87.78	4.38

Rådighedsfaktorer for danske kraftværksenheder mellem 100 og 199 MW

Kalenderår	59	60	61	62	63	64	65	66	67	68		
Alder af enhed											Gennemsnit for alle enheder	Akkumuleret gennemsnit
1	ASVB1	79	84	ASVB2	75	SVSB11	SHEB 2 VKEB 1	80	STVB 1 NEVB1	MKSB1	84	84
2				87	88	88	90	91	88	91	88	86
3					88	86	96	88	88	90	88	86
4						88	92	90	86	90	89	87
5							88	90	86	88	85	87
6								88	89	90	90	87
7									89	90	88	87
8										90	89	87
9										90	90	87

RELIABILITY ASPECTS OF SAFETY EVALUATION OF NUCLEAR POWER PLANTS

K. TAKEMURA*
Tokyo University of Mercantile Marine

S. HATTORI*
Chubu Electric Power Co.

1. Introduction

In 1958, we had been discussions on the reason why we did not need a container for a graphite moderated gas cooled reactor, for the construction project of Tokai nuclear power plant.

Soon later, the MITI** in Japan had made public a report on the safety evaluation of a nuclear power plant.

The report had envisaged the importance of the reliability analysis on the safety assessment of a nuclear power plant and furthermore a fault - tree like approach to follow a reactor accident step wise.

The CRESRES*** started its activity four years ago with the project purpose as following.

(1) To clarify the relation between the reliability of the safety system and reliability value of the system component.

(2) To study the basis of judgment for the safety of nuclear power plants.

This paper presents some interesting results obtained by the committee.

* Managing staff of the CRESRES

** Ministry of International Trade and Industry in Japan

*** Committee on Reactor Safety Evaluation and Reliability of Engineered Safeguard organized in Nuclear Safety Research Association.

2. Consideration of the Evaluation Basis on the Nuclear Reactor Safety

Recently, interest is increasing in discussions on the reliabilities of engineered safety features. But who could pronounce that present designs are suitable, not being over or less.

To obtain a proper target for the safety design of nuclear power plants or a reference value for the reliability of engineered safety features, the present effort of our committee is the first step of the approach.

It is extremely important for the human life in recent scientific civilisation to endeavour to establish a proper judgement basis not only on nuclear safety but also on industry safety.

Our committee has followed ordinary psychological process which general people experience when they have to judge the safety of a certain thing. Namely, we compared the risk of nuclear power with the various risks that surround us by using statistical data. "In what sorts of risks do we, human being, have daily life?" Survey activities to this question have been the first step of our works.

2 - 1 Risk study

We surveyed the various risks that surround us and followings are main survey data in Japan.

(1) Natural hazards

Severe natural hazards experienced in Japan are earthquake, typhoon and flood. The statistics over 60 years until 1965 shows that average death rate by the earthquake is 3×10^{-5} death/man year.

While the death rate by typhoon and flood is 1.2×10^{-5} death/man year.

(2) Disease

We obtained the disease death rate of the Japanese for each age rank from statistics;

age	disease death/man year	age	disease death/man year
0 ~ 4	4.7×10^{-3}	5 ~ 14	4.3×10^{-4}
15 ~ 24	4.4×10^{-4}	25 ~ 34	9.5×10^{-4}
35 ~ 44	2.0×10^{-3}	45 ~ 54	5.2×10^{-3}
55 ~ 64	1.4×10^{-2}	65 ~	6.4×10^{-2}

The risk of disease death changes by age. The disease death rate of the young age is decreasing year by year in Japan.

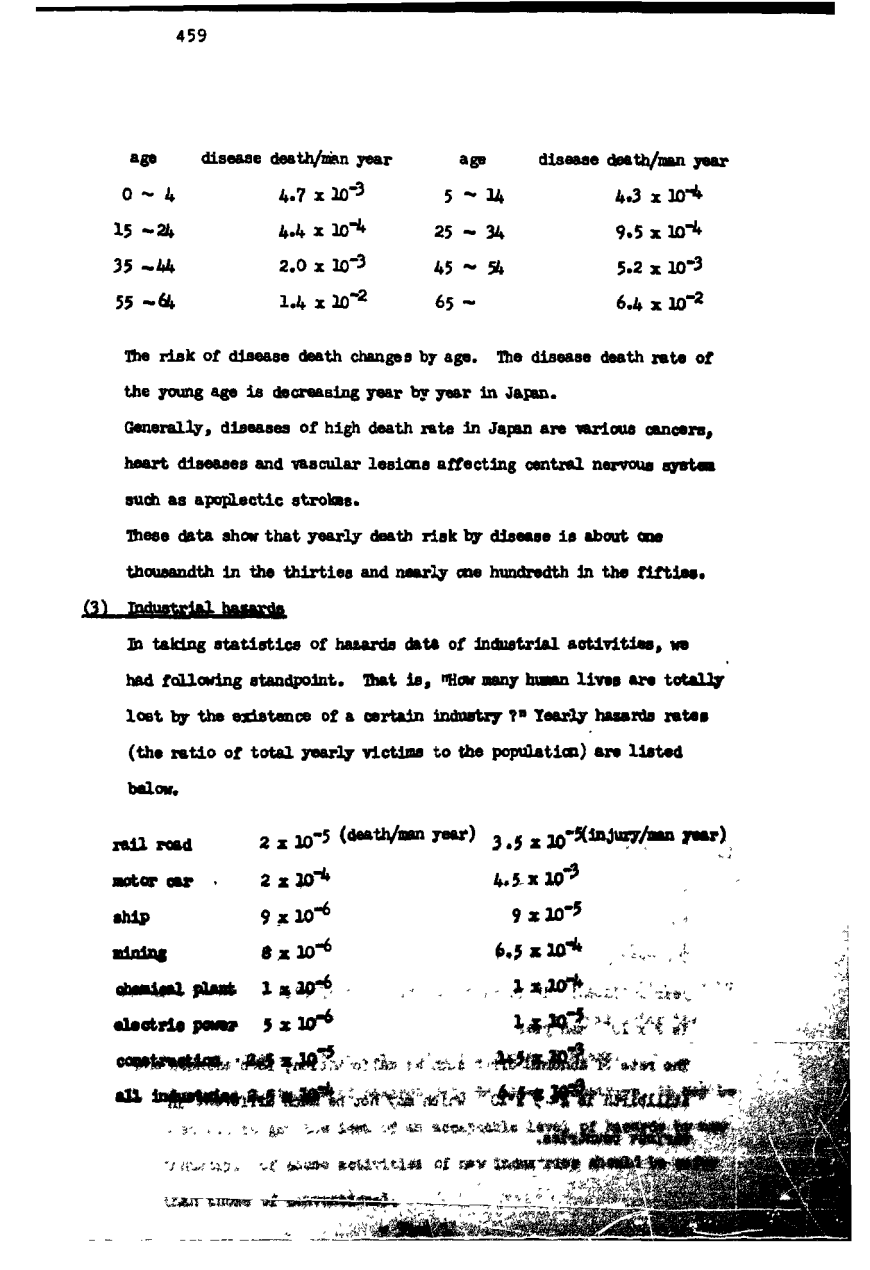
Generally, diseases of high death rate in Japan are various cancers, heart diseases and vascular lesions affecting central nervous system such as apoplectic strokes.

These data show that yearly death risk by disease is about one thousandth in the thirties and nearly one hundredth in the fifties.

(3) Industrial hazards

In taking statistics of hazards data of industrial activities, we had following standpoint. That is, "How many human lives are totally lost by the existence of a certain industry ?" Yearly hazards rates (the ratio of total yearly victims to the population) are listed below.

rail road	2×10^{-5} (death/man year)	3.5×10^{-5}(injury/man year)
motor car	2×10^{-4}	4.5×10^{-3}
ship	9×10^{-6}	9×10^{-5}
mining	8×10^{-6}	6.5×10^{-4}
chemical plant	1×10^{-6}	1×10^{-4}
electric power	5×10^{-6}	1×10^{-3}
construction	2.5×10^{-5}	1.5×10^{-3}
all industries	2.5×10^{-4}	4.5×10^{-2}



In treating statistics, we also paid some attention to devide people concerned into the following three parties;

the 1st party	:	people who are employed and at work for the industry concerned.
the 2nd party	:	people such as passengers of traffic facilities
the 3rd party	:	public in general

As for the question whether we should treat these parties separately or not, the conclusion of our Committee has not been reached as yet.

(4) Accidental risks of the public

Death rates of the public by all sorts of accidents are listed below.

motor car	2×10^{-4} (death/man year)
rail road	2×10^{-5} (")
ship wreck	1×10^{-5} (")
natural hazards	1×10^{-5} (")
others	1×10^{-4} (")
All sorts of accidents	4×10^{-4} (")

(5) Leukemia, thyroid cancer, abnormal birth

In relation to radiation hazards, special attention should be paid to leukemia, thyroid cancer, malformation, and stillbirth.

The yearly death rate by natural leukemia is 3×10^{-5} death/man year in Japan. It is said that the natural risk of thyroid cancer is 2×10^{-5} man year.

The rate of abnormal birth such as malformation, feebleminded and stillbirth is $4 \sim 5 \times 10^{-2}$ which may not be much different in various countries.

(6) Irradiation and its hazard

It is really difficult problem to get a risk value corresponding to a low level dose because of the lack of the information and of the uncertainty whether the hazard is caused by irradiation or not. Following the well known conservative assumption that the dose - effect curve is linear even below the irradiation level of 100 rem, one rem dose corresponds to the leukemia risk of 2×10^{-5} death/man year and the thyroid cancer risk of $1 \sim 2 \times 10^{-5}$ patient / man year. As for genetic effect, it is said that one rem dose gives the risk of $10^{-4} \sim 10^{-5}$ in relation to mutations and stillbirth. This figure is almost negligible compared with natural abnormal birth rate of 5×10^{-2}. Figure 1 shows our survey data in Japan.

2 - 2 Acceptable risk level

Industrial activities must be continued to accomodate more enhanced living standards. Then, in what extent should the "Safety" of those activities be pursued ? What is the target value of the safety design of the nuclear power plants ?

There may be following approaches.

A. Through the broad and profound survey, all sorts of risks surrounding our human being such as natural hazards, diseases and accidents can be studied scientifically, historically, geographically and sociologically.

Giving the analysis on the future status, and investigating the difference of those risks between circumstances, a reference value for the basis of safety evaluation would be set by finding the value adequately lower than those all sorts of risks.

B. Through the studies of hazards data in other industries, it may be possible to get the basis of an acceptable level of [illegible] industry. Of course activities of new industries should be safer than those of conventional.

C. In the case of the nuclear industry, it is a way to investigate the natural risks of leukemia, thyroid cancer and so on. Additional risk by nuclear industry should be adequately smaller than those risks of natural surroundings.

D. Safety and public hazards of a nuclear power plant could be discussed and judged in comparison with a conventional thermal power plant.

Let us apply our survey data to those sorts of approaches.

A. General human risk

The yearly disease deth rate is the smallest in the age from ten to thirty, and it is about 5×10^{-4} death/man year. The accidental risk of the public is different by year, by country and by circumstance. An average value of the accidental risk of the public is 4×10^{-4} death/man year.

B. Comparison with other industries

The figure, 2×10^{-4} death/man year, of car accidents is by no means acceptable. It is even a big problem to be solved as soon as possible. Then we take the figures 2×10^{-5} death/man year of rail roads, 2.5×10^{-5} death/man year of constructions and 5×10^{-6} death/man year of electric power as references.

C. Leukemia and malformation

The natural risk by leukemia is 3×10^{-5} death/man year in Japan. The natural abnormal birth rate of 5×10^{-2} is too big figure, which can by no means be a reference.

D. Comparison with thermal power plants

The figure 5×10^{-6} death/man year by the electric power industry is comparatively small. Besides, the contribution of the accidents of thermal power plants is very little in it. Then, let us think of the process to get the fuel consumed in the plant.

The hazards rate of coal mining people in Japan is one death/10^5 tons of coal product. A 500 MW coal burning power plant needs about 15 x 10^5 tones of coal to operate for one year. So, one year operation of a 500 MW coal burning power plant eventually consumes the fuel which is obtained by raising victimes of fifteen deaths and of more than one thousand injuries. This is too formidable present situation, so it is by no means allowed to take the figure as a reference. As for public hazards problems by burning fossil fuel in the ordinary operation of thermal power plants, we do not have quantitative conclusion yet.

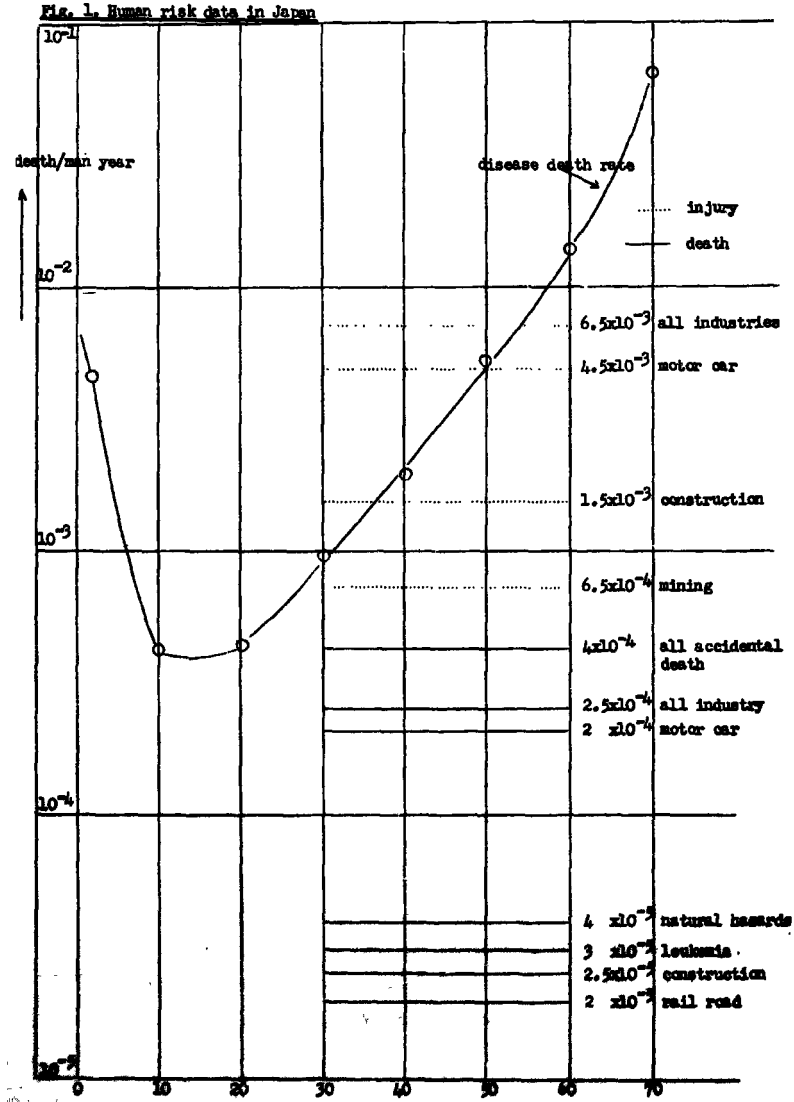
We have obtained a status reference figure of $10^{-6} \sim 10^{-5}$ death/man year, by means of general survey on natural risks and risks caused by industrial activities.

But when one comes to settle an acceptable standard value of the risk for the nuclear power industries, there are many important factors to be considered.

Therefore, the standard value might be some orders of magnitude less than the figure of $10^{-6} \sim 10^{-5}$ death/man year. We have to investigate these factors to be considered in between the standard value and the status reference figure.

We never forget to emphasize that the substantial effort of the safety assurance in the industrial activities must be continued endlessly for the prosperity of human being in the scientific age.

Fig. 1. Human risk data in Japan



3. Reliability Data of some Mechanical Components

The engineered safety features such as core spray systems and safety injection systems are not required to operate during the normal operation of plants, but are required to surely perform their functions in case of an accident. Therefore, in calculation of the reliability of their systems, it is reasonable to divide the duties into three categories, i.e. stand-by, start-up and operation. Reliabilities corresponding to the duties of these systems are derived from their failure data.

However, judging from the field data, we think it is impossible to separate the stand-by failures from the start up failures, because the stand-by failures can be discovered only at the time of next start.

The data of emergency diesel electric power generating facilities were obtained from the maintenance records and accident reports of Japan Broadcasting Corporation.

Resulting failure rates of 5KVA and 75KVA units are 6.9×10^{-3}/hr, 4.3×10^{-3}/hr during operation and 6.7×10^{-5}/hr, 5.6×10^{-5}/hr in stand-by condition, respectively.

3 - 1 Stand-by diesel electric power generating facilities

Japan Broadcasting Corporation had a failure survey of stand-by diesel electric power generating facilities to settle consistent maintenance system.

Capacities and numbers of these diesel units are 5KVA ~ 750KVA and 272 units, respectively, and 205 of those are 5KVA ~ 75KVA units.

We especially examined the failure data of these 5KVA (80 units) and 75KVA (52 units) facilities. Most of these facilities installed at relay stations.

These facilities were overhauled periodically by inspectors [illegible] control stations, and were inspected sometimes [illegible] power by inspectors of the local stations. [illegible]

overhauled or inspected once or twice a year. Moreover, automatic start-up testing had been done remotely from the local station once a month. These inspections were made following a check list in maintenance records, and this check list was composed of 114 components parts columns with five failure modes and three repairing treatments.

Operating hours, start-up times, repairing and miscellaneous were recorded on another sheet in maintenance records. In the case of a starting miss or a unpland stop, the details of the affair were mentioned on an accident report.

Table 1 and 2 show numbers of the failures of 5KVA and 75KVA units. In these Tables, "A" means a minor trouble, and "B" a serious failure. "B" failures are 10 - 20% of all troubles. There was no difference on the failure modes due to the lapse of time.

Failure rates during operation and in stand-by condition for 5KVA and 75KVA units are calculated from "B" failures, and they are shown in Table 3. The stand-by hours in Table 3 were obtained by substracting the operation hours from the calender hours. The judgement whether the failure had been occured during operation or in stand-by condition was made by checking up the maintenance records and the accident reports.

In general, a reliability of a stand-by facility is reasonably divided into three categories, namely reliability of stand-by duty, start-up duty and continuous operation duty. However, since the failures in stand-by period are discovered only at the time of next start, it is impossible to separate the stand-by failures and the start-up failures. Then we could not get the start-up failure rates, no matter how total start-up trials during two and a half years on 5KVA units and 75KVA units were 8389 times and 1346 times, respectively.

It is reasonable to think that the stand-by failure rates are affected by the stand-by hours, the environments and the extent of the maintenance.

It was shown that numbers of the failures per one unit-year regarding all troubles (A + B) of the 5KVA unit increased linealy with years. However, we could not get exact data to clarify the effects of stand-by hours and the other factors on failure rates. If the operator watched the facilities adequately, most of the deteriorating failures could be removed. However, most of these facilities had been unmaned, and a few deteriorating failures are included in Table 3. Table 4 shows the failure rates excluding deteriorating failures, so these failure rates depend only on chance failures. These failure rates in Table 4 are almost constant through the period surveyed.

Operation failure rate of $5\sim7 \times 10^{-3}$/hr and $1\sim2.5 \times 10^{-3}$/hr in Table 3 and 4 are rather large compared with operation failure rate of about 3×10^{-4}/hr which was obtained from our another survey on merchant marine dynamo engines. It can be said that the difference of these failure rates depends on the different maintenance system.

Table 1. Failure of 5KVA units

Inspection year		F1963		L1963		F1964		L1964		F1965		Total	
Numbers of unit		9		12		29		11		19		80	
Failure grade		A	B	A	B	A	B	A	B	A	B	A	B
Components	Engine main parts	26	5	22	2	53	9	15	1	67	19	183	36
	Fuel oil system	13	2	4	1	34	2	5	0	21	1	77	6
	Lub. oil system	6	0	0	0	23	0	4	0	14	0	47	0
	Cooling water system	1	1	1	1	4	1	0	0	7	0	13	3
	Starting cell motor gear sys.	10	0	0	2	16	1	1	0	14	0	41	3
	Safety device sensor	0	0	0	0	2	0	0	0	2	0	4	0
	Safety device relay & meter	4	1	0	0	7	0	2	2	2	3	15	6
	Engine bed & foundation	4	0	0	0	2	0	0	0	4	0	10	0
	Engine stop mech. & FO, LO, CW supply system	9	6	1	1	6	6	2	0	18	2	36	15
	Gas exhaust system	0	0	0	0	0	1	0	1	0	0	0	2
	Auto switching system	0	2	0	1	2	2	0	1	0	4	2	10
	Miscellaneous	2	0	3	0	0	1	0	1	0	0	7	2
T o t a l		75	17	31	3	149	23	29	6	149	29	433	83
Failures per unit		8.3	1.9	2.6	0.7	5.1	0.8	2.6	0.5	7.8	1.5	5.4	1.04

F,L : First half, Last half of the year

F O : Fuel oil

L O : Lubricating oil

C W : Cooling water

Table 2. Failure of 75KVA units

Components	Inspection year	F1963		L1963		F1964		L1964		F1964		Total	
	Numbers of unit	21		1		20		6		4		52	
	Failure grade	A	B	A	B	A	B	A	B	A	B	A	B
	Engine main parts	28	4	1	0	34	3	10	1	16	0	89	8
	Fuel oil system	6	0	0	0	5	0	0	0	0	0	11	0
	Lub. oil system	5	1	0	0	7	0	1	0	1	0	14	1
	Cooling water system	3	0	0	0	2	0	0	0	1	0	6	0
	Starting cell motor gear sys.	4	1	0	0	2	0	0	0	2	1	8	2
	Safety device sensor	3	0	0	0	0	1	0	0	0	0	3	1
	Safety device relay & meter	17	0	0	0	5	1	1	0	2	0	25	1
	Engine bed & foundation	1	0	0	0	0	0	0	0	0	0	1	0
	Engine stop mech. & FO, LO, CW Supply system	8	2	2	0	7	0	0	0	3	0	20	2
	Gas exhaust system	0	0	0	0	0	2	1	0	1	0	2	2
	Auto switching system	2	0	0	0	0	0	0	0	1	0	3	1
	Miscellaneous	0	0	0	0	0	0	0	0	0	1	0	0
	T o t a l	76	8	3	0	62	7	13	1	27	2	181	18
	Failures per unit	3.6	0.4	3.0	0	3.1	0.4	2.2	0.2	6.8	0.5	3.5	0.35

F, L : First half, Last half of the year

F O : Fuel Oil

L O : Lubricating oil

C W : Cooling water

Table 3. "B" failure rates of 5KVA and 75KVA units in stand - by, start - up conditions and during operation

		In stand-by • start-up conditions						During operation						Start up No.s
	Year	A hr	B hr	C Nos	D Nos	C/A	D/B	A hr	B hr	C Nos	D Nos	C/A	D/B	
5 KVA	F 1963	38510.8	38510.8	8	8	2.07×10^{-4}	2.07×10^{-4}	1017.2	1017.2	9	9	8.7×10^{-3}	8.7×10^{-3}	1283
	L 1963	57218.5	89729.3	3	11	5.86×10^{-5}	1.12×10^{-4}	1397.5	2414.7	4	13	2.86×10^{-3}	5.4×10^{-3}	1858
	F 1964	125570.7	215300.0	7	18	5.58×10^{-5}	8.35×10^{-5}	1797.3	4212.0	14	27	7.8×10^{-3}	6.41×10^{-3}	1759
	L 1964	46742.1	262042.1	1	19	2.14×10^{-5}	7.25×10^{-5}	1305.9	5517.9	4	31	3.05×10^{-3}	5.62×10^{-3}	1215
	F 1965	81333.4	343375.5	4	23	4.91×10^{-5}	6.71×10^{-5}	2114.6	7632.5	22	53	5.95×10^{-3}	6.95×10^{-3}	2274
	Total	343375.5		23			6.71×10^{-5}			53			6.95×10^{-3}	8389
75 KVA	F 1963	9046.0	9046.0	3	3	3.31×10^{-5}	3.31×10^{-5}	771.0	771.0	5	5	6.48×10^{-3}	6.48×10^{-3}	496
	L 1963	4313.0	13359.0	0	3	0	2.24×10^{-5}	55.0	826.0	0	5	0	6.05×10^{-3}	27
	F 1964	86868.9	100227.9	4	7	4.6×10^{-5}	$7. \times 10^{-5}$	971.1	1797.1	3	8	3.08×10^{-3}	4.45×10^{-3}	492
	L 1964	25938.8	126166.7	0	7	0	5.55×10^{-5}	169.2	1966.3	1	9	5.91×10^{-3}	4.58×10^{-3}	153
	F 1965	17404.7	143571.4	1	8	5.75×10^{-5}	5.57×10^{-5}	163.3	2129.6	1	10	6.12×10^{-3}	4.7×10^{-3}	178
	Total	143571.4		8			5.57×10^{-5}	2129.6		10			4.7×10^{-3}	1346

Note; A : Stand-by hours or operating hours
B : Cumulative stand-by hours or operating hours
C : Number of failures
D : Cumulative number of failures
C/A : Failure rates per hr.
D/B : Cumulative failure rates per hr.

Table 4. "B" failure rates excluding deteriorating failures

	5KVA	75KVA
In stand-by · start-up conditions	1.76×10^{-5}/hr	3.48×10^{-5}/hr
During operation	1.18×10^{-3}/hr	2.34×10^{-3}/hr

3 - 2 Reliability data in JPDR

JPDR(Japan Power Demonstration Reactor) is a natural circulation, direct cycle BWR plant with 12,500 KWe electricity generation.

(1) Troubles influencing on continuous operation

Troubles influencing on continuous operation of JPDR from March 1965 to February 1967 were as follows :

unscheduled shutdown	22
(scheduled shutdown	10)
start-up delay	7

It is seen that the scheduled shutdown of the plant was only 30 percent, though this figure is much improved at present.

The classes of troubles which gave plant shut-downs are shown in Table 5. Leakage of steam or water from the primary coolant system was observed eight times and this corresponded to almost one third of shutdown causes. Failures of components and malfunctions of components caused plant shut down seven and four times, respectively. It is noted that the rupture of diaphram valves in the scram air system was avoided after the inspection intervals had been lengthened from once a day to once a week.

In Table 6, the causes of seven start up delays of the plant during the above period are shown. Four of them are caused by the leakage from the primary coolant system.

(2) Maintenance records of JPDR

In review of maintenance records of an electricity generating plant, the concern is not with calendar days or accumulated hours of reactor operation, but with accumulated hours of electricity generation, because it could be said that almost hundred percent of components were put in service during this period.

The relations between the accumulated hours of electricity generation and the numbers of maintenance sheets are shown in Fig. 2, regarding mechanical, electrical and instrument component, respectively. Total numbers of maintenance sheets are also shown. Stepwise increases of failures at 2,200, 4,400, 5,200, 7,400 and 9,900 hours correspond to the periodic inspection of the plant or refueling work and so on. It can be said that the number of failures are nearly proportional to the accumulated hours, if failures during only power generation are picked up, and initial failures are excluded. Total failure rates of component groups are derived as follows, based on the slope at the end of each curve shown in Fig. 2.

mechanical component	1.0
electric component	0.2
instrument	1.4
total	2.6

(unit : failures/days of power generation)

Dominate causes of these failures are (1) water leakage from valves (8.1 failures/month), pumps (4.1 failures/month) in mechanical components, (2) failures of motor control panels or annuciator panels (4.5 failures/month) in electric components and (3) calibration or readjustment of nuclear and process indicators, controllers in instrument components. It could be considered that the failure mode of most components is a random failure, excluding initial 1,000 hours.

(3) Failure data of components in JPDR

Trial to review the reliability of the emergency cooling system in JPDR had been made to survey which component was dominant for the reliability of the system. 2)

The data of failure rates used to evaluate the system reliability were shown in the last report. Some of them were derived from the maintenance record of JPDR during 27 months from July 1964 to September 1966, and expressed in the form of failure per unit time or unit action. In Table 7, failure numbers of the main components of the system are shown. Judging from the number of failure samples, derived failure rates shoud include considerable statistical deviation, and high confidence level can not be expected. But it can be said that the overall reliability of an emergency cooling system is much dependent on the operation reliability of motor driven valves. To get a more useful failure rate on a motor driven valve, operation counters have been installed to both relays for open and close valves. Numbers of valves whose operation are counted are as follows.

DC motor valves	25
AC motor valves	28

The number of counts is recorded every week in check sheets, with respect to all valves. When some abnormal situation is found at either open or close action of a valve, operation people or maintenance people should describe the situation and repairing work in detail. After preliminary examination of the counters, the failure rate of a motor driven valve was obtained from the data for one year (up to March 1969). Recorded faulty operations of a valve are two for close close action and zero for open action. The total counts of close action were 1967, which give the failure rate for close action

$$\lambda_c = \frac{2}{1967} \approx 1.0 \times 10^{-3} \text{ failure/close.}$$

The confidence level of this figure can not be discussed because the number of failure sample is very small for statistical treatment. It is hoped that this kind of survey would be continued for longer time, for instance, five years, to obtain more reliable informations.

Table 6. Causes of start-up delay

CAUSES	NO. OF CAUSES
Failure of CIC Range Switch	1
Displacement of Limit Switch for Scram Valve	1
Abnormal Indication of Reactor Level meter	1
Rupture of Disphram Valve in Scram Air System	1
Leakage through Valve on Core Spray System	1
Water Leakage from Cool System of In-core Monitor	2
Total Delay	7

Table 5. Causes of plant shutdown

CAUSE OF TROUBLE		NUMBER	REMARKS
Leakage of Steam or Water from Primary System	steam leakage from the root valve of reactor level gauge	2	
	steam leakage from the valve on core spray system	3	
	water leakage from a union of seal coolant of control rod	1	
	steam leakage from a drain line of MSV	1	
	water leakage from incore monitor cooling system	1	
Malfunction of Component	turbine trip from malfuction of MSV	1	Scram
	malfunction of primary bypase valves	1	Scram
	malfunction of period meter	2	Scram
H_2 leakage	rupture of valve diaphram on scram air system	3	Rod Run In
Strainer Blockage	low suction pressure of FWP	1	Scram
	air inflow to condensate during replacing strainer	1	Scram
Mis-Operation	high condenser pressure during start-up	1	Scram
Component Failure	MSV stick	1	
	fault contact of operation mode switch	1	Scram
	low pressure on oil system for primary bypass valves	1	
	rupture of diaphram in off-gas compressor	1	

Table 7. Failure Mode from Maintenance Record

ITEM	MODE OF FAILURE		FAILURE RATE	REMARKS
Failure of Motor driven Valve in open operation (38)	1) thermal relay tripped from packing hardening	2	$\frac{9 \text{ (failures)}}{1650 \text{ (opens)}} = 5.4 \times 10^{-3}$ *	
	2) motor control center burnt	2		
	3) fuse melting in control circuit	2		
	4) terminal loosened in control circuit	1		
	5) insufficient adjustment of torque switch	1		
	6) failure of auto-manual switch	1		
	total	9		
Failure of Motor driven Valve in close operation (38)	1) thermal relay tripped from packing hardening	2		
	2) insufficient adjustment of torque switch	3		
	3) failure of contactor in control circuit	2		
	4) DC system ground	1		
	5) others	1		
	total	9		

ITEM	MODE OF FAILURE		FAILURE RATE	REMARKS
Failure of Engine for Pump (4)	1) failure of relay contact (for start-up duty)	3	start up duty $\frac{3\text{ (failure)}}{306\text{ (start)}} = 9.8 \times 10^{-3}$ *	
	2) terminal to battery loosened (for stand-by duty)	1	operation duty $\frac{1\text{ (failure)}}{1000\text{ (hrs.)}} = 1.0 \times 10^{-3}$ **	same to diesel generator
	total	4	stand by duty $\frac{1\text{ (failure)}}{77952\text{ (hrs.)}} = 1.3 \times 10^{-5}$ **	
Failure of Level Switch (17)	1) DC system ground	1		
	2) deviated indication during plant restart after scram	1	$\frac{2\text{ (failure)}}{331296\text{(hrs.)}} = 6 \times 10^{-6}$ **	
	total	2		
Failure of Power System (1)	1) thunder	4		
	2) earthquake	1	$\frac{10\text{(failure)}}{19488\text{(hrs.)}} = 5.1 \times 10^{-4}$ **	
	3) others	5		
	total	10		

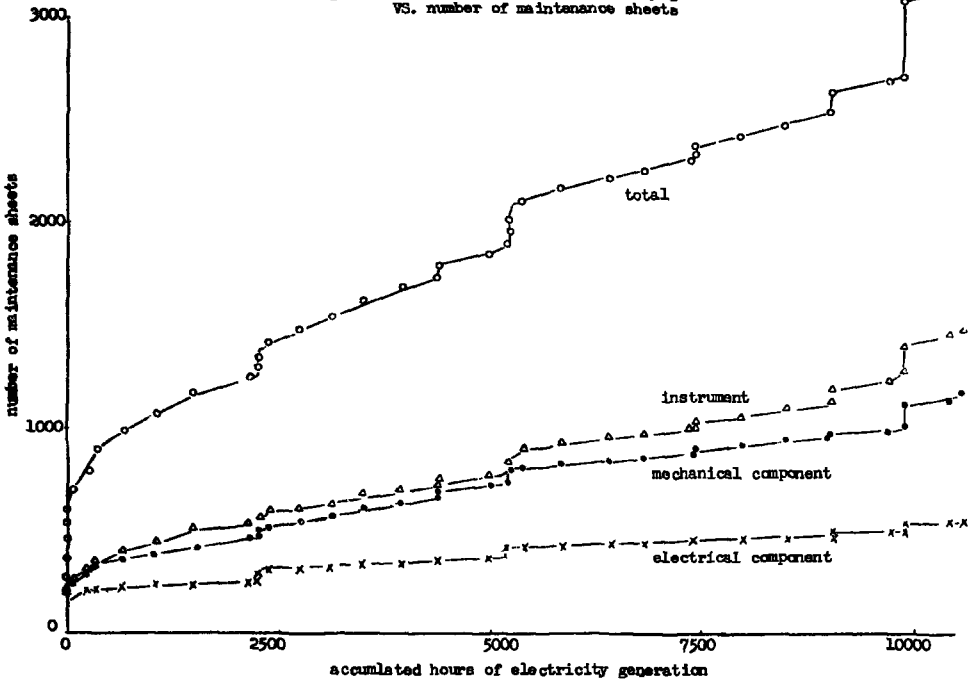
Note:

(a) * failure rate depending on number of actuation

(b) ** failure rate depending on time

(c) numbers of subject are shown in parenthesis in "ITEM"

Fig. 2. Accumulated hours of electricity generation VS. number of maintenance sheets



4. Conclusion

An approach for the safety evaluation basis, reliability data of mechanical components, these subjects presented here are topics of our committee.

Our committee will continue the activities for the work to establish a probabilistic procedure on the safety evaluation of the nuclear power plant, along with the work for the collection of the failure data of various components concerning nuclear safety.

(Reference)

(1) YAMADA, T., Safety Evaluation of Nuclear Power Plant, Proc. IAEA Symposium (1962, 493)

(2) TAKEKOSHI, T., Reliability Assessment of Engineered Safeguards of Nuclear Power Plants. Second CREST Meeting, Ispra, June, 1968.

(3) I.C.R.P. Committee No.1, "The Evaluation of Risks from Radiation" I.C.R.P. Publication 8, Pergamon Press (1966)

COMMISSION OF THE EUROPEAN COMMUNITIES

8322/XII/69-E

Directorate General
General Research and Technology

Directorate General
Industrial Affairs

RELIABILITY CONSIDERATIONS FOR MECHANICAL COMPONENTS OF CONTROL ROD DRIVE SYSTEMS OF GAS-COOLED POWER REACTORS OPERATED IN THE EUROPEAN COMMUNITY

by

J. EHRENTREICH

H. MAURER

presented at the

Meeting of Specialists on the Reliability of Mechanical Components and Systems for Nuclear Reactor Safety

Risø, 24th - 26th September 1969

8322/XII/69-E

RELIABILITY CONSIDERATIONS FOR MECHANICAL COMPONENTS OF CONTROL ROD DRIVE SYSTEMS OF GAS-COOLED POWER REACTORS OPERATED IN THE EUROPEAN COMMUNITY

Summary

Different principles adopted by various suppliers of mechanical parts for control-rod drive systems in gas-cooled power reactors operated in the European Community are described on a comparative basis. The function of the different systems is demonstrated by reliability block diagrams and the reliability analysed for both normal and scram mode of operation.

The following subjects are treated in details

1. Estimation of possible failure rates of mechanical system components. Comparison of the analytically determined inherent system reliability with the operational system reliability.

2. Reliability analysis of the complete control and safety systems (total number of control and safety rods), on the basis of the analysis of individual rod drives.

Contents

1. CONTROL ROD DRIVE MECHANISMS FOR GAS-COOLED POWER REACTORS

In gas-cooled power reactors more than 100 long (8–10 m) and heavy (50–500 kg) control rods are moved in hot gas. A drum and cable or a sprocket and chain arrangement is used in the drive mechanism system. The power chain to operate the drive mechanism is composed of an electric motor and a gear system, but even a pneumatic operated piston has been used to rotate the cable drum via the corresponding gearing (Ref. 2).

At first cables were utilised to lift or to lower the control rods. Later, in England, because of increased control rod weight and insertion velocity with the more sophisticated Magnox stations (e.g., Dungeness, Sizewell, Oldbury and Wylfa), the cables were replaced by chains.

Three control rod drive mechanisms of different designs used for the EDF-2, the EDF-3 and the Latina reactor have been chosen for an analysis to evaluate data characterizing their operational reliability.

2. DESCRIPTION AND ANALYSIS OF CONTROL ROD DRIVE SYSTEMS FOR RELIABILITY CONSIDERATIONS

2.1. The EDF-2 Reactor Control Rod Drive Mechanism

The French EDF-2 plant at Chinon is equipped with a CO_2-cooled power reactor. Individual cable and drum mechanisms installed in a pressure casing are used to raise or to lower the 104 absorber rods in the reactor core (Figs. 1 and 2).

A pneumatic and mechanical system is employed to drive the cable drum. Power to rotate the drum is obtained from a pneumatic cylinder which is actuated by the differential pressure between the CO_2 blower and the reactor core. The actuated movement of the piston rod is transferred into drum rotation by a differential gear and a set of bevel gears and shafts.

Two sprung-set, pneumatically released, drum-type brakes are incorporated in the drive mechanism. Their functions are the following:

- to keep the rod in a given position
- transformation of alternative rack movement into continuous rotation in one direction or the other
- realisation of a controlled rod drop.

Piston movement is transmitted to the mechanism by the rack (1) (Figs. 3 and 4). The mechanism is linked to the drum by the intermediate gearing (4). The different rod movements are carried out with the two brakes FA (2) and FB (3).

The rack (1) rotates the sector (6) supporting shaft (11) of the satellite which is geared into the gear rim (10), which rotates the drum by the intermediate gearing (4). The gear rim (10) is also geared into sector (6) via sector (8), the satellite pinion (9) and the conical pinion (7). A centrifugal friction regulator (13) with the governor weights fixed to (5) rubs on the inner surface of (10) and limits the rod drop velocity to 2 m/s.

Rod operations:

- Rod lifting

  Each piston stroke corresponds to an elementary rod movement of 10 cm called a "quantum". The change of action of the two brakes allows a continuous rod movement with alternating piston movement. The time necessary for a 10 cm elementary movement is 0.6 s.

- 1a Direction A of piston (fig. 7) brake FA (2) set, brake FB (3) open.

  When brake (2) is set, the whole shaft (5) is blocked. The rack (1) drives the sector (6) and by means of the pinion (7) the sector (8) in the opposite direction. Sector (8) drives satellite-pinion (9), which rolls on the blocked pinion on shaft (5) and in this way drives the gear rim (10), i.e., the drum also, so that the control rod is lifted.

  When the piston reaches the highest position, the brake FA (2) is opened and the brake FB (3) is set. The brakes are operated by electric valves.

- 1b Direction B of piston

  The brake FB (3) is set and hence the brake pulley (12) blocked. The rack (1) drives the sector (6) in the opposite direction in relation to movement 1a. The shaft (11) rolls on (12) blocked and drives the gear rim (10) in the same direction as in case 1a.

- Rod insertion

The rod is moved downwards in the same way as when lifted, the only difference being that the brake action is inverted, e.g.,

piston in direction A	brake FB (3) set.
piston in direction B	brake FA (2) set.

- Controlled rod drop

Rod drop is caused by cutting the power supply to the electric valves. Both brakes are released and motor action is no longer possible. The motor piston is still moving to its highest or deepest position.

The control rod rotates the drum by its weight, which means that the gear rim (10) also turns. Then, by means of the satellite-pinion (9), the shaft (5) is rotated with the centrifugal regulator (13) which is fixed to it. The speed of (5) and (13) is much higher than in normal operation, so the regulator weights move outwards and start to rub on the drum (10), thus stabilising the movement; (10) and (13) rotates in the opposite direction. Rod braking and stopping at the end of the rod travel is performed by setting brake FB (3).

The order to brake FB (3) is given by a contact, which closes when the rod reaches a predetermined position.

- Resting position

In the resting position the rod is fixed, possibly in an intermediate position. In this case there is not air supply to the pneumatic motor and both brakes FA (2) and FB (3) are applied. The weight of the rod tries to turn the gear rim (10). The gear rim (10) [illegible] sector (5) by means of the satellites (11) [illegible] are themselves geared in (5) and (12), in two [illegible] so that rod blocking is assured.

All parts of the mechanism are housed inside a pressure casing, which is divided into three parts

- the upper part contains the electric valves (pressure : reactor pressure + 10 b)
- the middle part contains all the components of the mechanism (pressure : reactor pressure)
- the lower part contains the drum (pressure : reactor pressure).

The middle part can be opened for maintenance purposes. Leaktightness between this and the lower part is ensured by an adjustable double rotary gas seal on the drive shaft between the gear rim and the cable drum.

The lower part of the control rod drive mechanism is installed in a sleeve tube fixed to the reactor pressure vessel. The pressure casing with the drive mechanism is supported by the upper part of the sleeve tube. Leaktightness is guaranteed by a flange seal (Figs. 1 and 2).

The control rod dimensions are:

active length (12 parts)	6.714	m
total length	7.016	m
maximum diameter	68	mm
weight	36	kg

The control rod is fixed to a cable and consists of 12 cylindrical absorber parts interconnected by hinge couplings and another cable (safety cable) (Figs. 5 and 6).

Two types of control rods are available: black and grey ones. The black ones use boral (boron/aluminium carbide) and the grey ones stainless steel as the absorber material.

The control rod moves in a graphite channel. A separate damper is installed on the core support plate.

The position indication system comprises:

- a pinion mounted on the shaft (item 4)
- a screw and a wheel geared in the pinion mentioned
- a runner on the screw to close final position contacts and the contact for brake setting
- a selsyn driven by a system of wheel and endless screw connected to the above-mentioned screw. The selsyn is used to indicate rod position - the total rod travel corresponds to 346°.

Cable rupture is indicated by the slack cable switch.

Fig. 8 shows a block diagram for a EUF-2 reactor control rod drive unit drafted for the following reliability considerations. Estimated failure rates for the different parts have been included.

2.2. The EDF-3 Reactor Control Rod Drive Mechanism

The EDF-3 control rod drive mechanism consists of an electric motor winch mounted on the upper part of the biological shielding plug (Fig. 9).

Each winch is composed of

a power chain with
motor (3 phase asynchronous) with brake (closed when not under tension) and speed limit device, reduction gear, differential gear and drum

a security chain with
drum, differential gear, speed regulator and disc brake and its control

a transmission chain with
drum, cables, slack cable control, cable guide and connecting link

a position reproduction chain with
gears, cam crown, selsyn (self-synchronized motor) and microswitches

and auxiliaries.

The gear by which motor rotation is transmitted to the drum is composed of

- a double reduction gear train between the motor shaft and the differential gear shaft with the pinion (item 3) (see Fig. 10)
- a differential gear with a rim (item 4) which can be fixed by the brake (item 13) (of the safety chain), a central pinion (3), an intermediate (satellite) differential wheel (5) and a satellite carrier (6).

- the junction between the differential gear and the drum, consisting of a pinion (7) driven by the satellite carrier (6), a shaft and a bevel gear (8) to transfer motor movement to the drum (9).

These parts belong to the power chain.

Rod operation

- rod stop (Fig. 11)
  both brakes are closed, the motor brake is closed automatically because there is no tension and the gear disc brake is closed electrically. Therefore pinion (3), rim (4) and satellite (5) can not move and the drum and the control rod are blocked.

- normal operation (Fig. 12)
  The control rod is lowered or lifted by changing the direction of motor rotation.
  The disc brake (of the safety chain) rests set electrically (as stated above).
  The motor brake is open because motor and brake are under tension.
  Operating are
    the double reduction gear (2), the pinion (3), the satellite (5) rolling on the rim (4), blocked by the safety brake (13), the satellite-carrier (6), the transmission gear (7, 8) and the drum (9).
  Normal rod velocity is 15 cm/s.

When in case of an electrical supply failure rod movement is required, the control rod drives the motor by its weight and via the drum and the power chain.
The motor speed is limited by a centrifugal speed limit device to 1500 rpm. When the motor receives the stop signal the motor brake stops the control rod.

The safety chain is composed of

- the junction between the differential gear and the drum (see description of the power chain) and
- a rod drop speed control device with the satellite carrier (6), the satellite pinion (5) and the rim (4), on which are fixed:
  a centrifugal regulator (12) (the regulator weights rub on the surface of the stationary casing)
  a disc of the brake (13) and the brake shoes (with Ferodo linings) to brake both sides of the disc.

The disc brake is set electrically in normal operation and mechanically at the end of the control rod travel.

The safety chain is used to scram the reactor. The motor brake is set (because there is no supply tension) and the safety brake is released because there is no power supply to the coil (15) (no tension).

Then the drum drives the satellite-carrier (6) over (8) and (7).

The pinion (3) is blocked by the motor brake, on which the satellite (5) rolls rotating the planetary gearing (4).

The weights of the centrifugal regulator device fixed on the planetary rim start to rub on the surface of the gear casing. Control rod speed is limited to 2 m/s; the starting acceleration is 0.5 m/s^2.

At the end of the rod travel a cam on a rim of the position reproduction chain acts on a shaft, which closes the safety brake and stops the control rod.

The control rod cable has a diameter of 4.8 mm and consists of seven cordons of seven wires each 0.5 mm in diameter.

The selsyn (item 21, Fig. 10) of the position reproduction chain is driven by the cam crown (20) and gives the exact rod position at any moment. The rotor of the selsyn is supplied with 127 V, 50 Hz current and turns 346° between the two extreme rod positions.

A total of 138 control rods are available to ensure safe operation of the ZDF-3 reactor.

The motor winch is installed in the upper part of the biological shielding plug (Fig. 9).

The control rods have an outer diameter of 62 mm, a total length of 7354 mm (7203 mm active length) and a weight of 40 kg.

There are 75 "grey" and 63 "black" rods. Black rods contain boron carbide but grey rods only stainless steel as the absorbing material.

The active part of the control rod is composed of nine elements with a length of 765 mm each. The elements are interconnected by hinge couplings. For safety reasons a continuous cable is also fitted.

A separate damper is available for each control rod on the core support plate.

The working conditions of a control rod drive mechanism and the control rod in its graphite channel are:

CO_2 pressure 30 b (nominal 25 b)

temperature mechanisms 80 - 120°C
control rods 400°C
shock absorbers 225°C

coolant flow 300 g/s CO_2 at 240°C

max. neutron flux 4 10^{13} n/cm^2 s

Fig. 15 shows a block diagram for the following reliability studies on control rod drive mechanisms for gas-cooled power reactors including the EDF-3. Estimated failure rates for the different items of the unit are indicated.

2.3. The Latina Reactor Control Rod Drive Mechanism

The Latina reactor control rod drive mechanism consists essentially of a motor-driven, geared chain winding drum, housed in a pressure casing (Figs. 16 and 17, item 5).

A permanent magnet induction (eddy current) brake is fitted co-axially to the upper end of the motor shaft (item 4).

The weight of the control rod is entirely supported by the motor torque, whether the motor is moving or stationary.

The driving motor of the normal induction type, is designed for three-phase low frequency supply. Changes in control rod speed and direction are simply carried out by varying the rod motor supply frequency and reversing its polyphase rotation. At zero frequency the rod motor remains stationary, holding the rod suspended in the required position.

When it is desired to initiate a reactor trip the motor-windings are de-energised and the torque at the drum, because of the rod weight, is then sufficient to accelerate the moving parts to allow the control rod to fall into the reactor core from any withdrawn position.

A freewheel device (item 7) is included to prevent reverse winding of the chain if the motor continues driving after the rod has reached the fully lowered position.

A winding gear (item 8) connects the motor shaft with the chain drum (item 9).

The rod end of the chain is passed over a spring loaded pulley, the movement of which operates a microswitch in a slack chain indicator device. The pulley also drives a geared rod position transmitter. ../OC.

The pressure casing of the control rod actuator is of welded construction. All joints have double O-ring seals and provision is made for testing the inner seal where required.

The upper cap of the pressure cover can be removed to allow attachment of a hand winding gear.

The control rod consists of a number of absorber inserts (the active position) between a liner and a sheath. The rod is approximately 8 m long and its weight is approx. 120 kg. It is suspended by a chain from the actuator and is restrained sideways by a guide tube extending between the actuator standpipe and the core plate. The reactor is equipped with 100 control rods.

The inserts are ferro-boron sintered compacts in the form of hollow cylinders with an outer diameter of $\sim$75 mm, an inner diameter of 62 mm and $\sim$ 25 mm long. They are stacked to form an active length of 7 m with a boron content of $\sim$0.58 kg/m.

The sheath is a seamless 18/8 stainless steel tube, and a thin stainless steel liner is fitted on the inside to keep the inserts in position should spalling occur in service.

If the control rod hoist chain fails, the emergency arresting device incorporated at the lower end of the rod would bring the rod to rest without damage to permanent reactor components. The arresting device is capable of absorbing the energy in a drop from the fully withdrawn position plus one accidental drop during subsequent recovery from the reactor.

The clearance between the control rods and the channels has been determined for the worst conditions of differential movement due to pressure vessel and core temperature, gas pressure and core distortion.

In no case is the clearance zero. But even if the effective clearance were to become reduced to zero in some of the channels by accident conditions, the inherent flexibility of the control rods should still permit full insertion. The guide tubes between the standpipes and the top of the core prevent any tendency for the control rods to jam in the event of a top duct branch failure causing lateral gas loadings in the pressure vessel top dome space.

Accelerated life tests have been carried out on the control rod actuators, *e.g.*:

raising and lowering : 0 - 27 ft travel
minimum specified 80 operations, equivalent to four start-ups and shut-downs per year for 20 years
actual number of tests carried out (for Bradwell) 306

rod emergency trip : 27 ft to 0 travel
minimum specified 160 operations, equivalent to eight trips per year for 20 years
actual number of tests carried out (for Bradwell) 462

hunt test at 27 ft
the load on the mechanism is the maximum and is continuously oscillated through $\sim$ 14 mm; minimum specified 500,000 operations,
actual number of tests carried out (for Bradwell) 511,174 operations.

auto control test at 13 ft
the control rod is oscillated at $\pm$ 200 mm above this point,
minimum specified operations 500,000,
actual number of tests carried out (for Bradwell) more than 500,000.

From the results of the Bradwell accelerated life tests it was concluded that any wear occurring in the actuators will not affect their trip reliability or other aspects relating to reactor safety.

The actuator moving parts are of corrosion resistant material; and other ferrous parts are protected by epoxy resin metal-free paints (e.g., the pressure casings). High-temperature lower standpipe parts which are not corrosion resistant are coated with colloidal graphite.

Corroding conditions become significant only during reactor start-up with a fresh charge of carbon dioxide and higher than normal water and oxygen content.

Life tests in moist carbon dioxide on actuators are performed in an atmosphere of commercial-grade bottled carbon dioxide at $\sim$ 10 atü (moisture content normally 400-300 ppm by weight).

No evidence of corrosion or of deterioration of surfaces and finishes (other than by mechanical wear of rubbing parts) has been found. No seizing of chain links was observed. No significant changes in the resistances of windings or of the insulation were found.

The rod position indication system consists of a selsyn transmitter in each mechanism which rotates 320° mechanical for the total control rod travel. The transmitter is directly geared to the rod chain without slip. The backlash in the gears is small. Each actuator transmitter is directly connected to its individual rod position receiver which it drives as a slave (positional error 0.5° mechanical).

Fig. 19 shows a block diagram for reliability studies on the Latina control rod drive mechanism. Estimated failure rates on the unit components are indicated.

3. RELIABILITY ANALYSIS OF CONTROL ROD DRIVE SYSTEMS OF GAS-COOLED POWER REACTORS

3.1. Failure Rate Estimation of Control Rod Drive Unit Components

The failure rates (see Table 1) used for the reliability analysis are based on an operating time of 10^6 reactor hours. No defect statistics for the drive systems investigated were available, so the failure rates were estimated on the basis of experience with similar components employed in other branches of industry. In no case was it possible to examine the criteria on which the failure rates were based. For this reason the empirical data taken from the literature (Refs. 8 and 9) are subject to a high margin of uncertainty.

The analysis performed is not intended to give a quantitative assessment of the reliability of the different control rod drive systems. It may only be considered as a comparison of the reliability of the three different systems chosen. The failure rates of those components which are used in all three systems are therefore of no importance for the comparison.

3.2. Reliability Analysis of Individual Control Rod Drive Units

The results of the numerical analysis are listed in Table 2 and are based both on weekly inspection cycles of the control rod drive units and on quarterly ones in order to demonstrate the importance of the inspection period, mainly for units which are not continuously in operation, such as the bulk and scram rods.

The analysis was performed for the mechanical system components only and can therefore not be regarded as complete. For a complete reliability analysis all the parts of a system must be taken into account, i.e., the mechanical part as well as the electrical and electronic parts, and the human factor should be included too. The consideration of the human factor is of importance for safety systems where incorrect action by an operator can be a contributing factor in respect to system failure, especially in the case of a completely manual safety system where an operator's action could directly lead to failure of the system.

The results of the analysis show that the Latina control rod drive system seems to be somewhat more reliable (see Table 2) than the two EDF-control rod drive systems, this being possible because of its uncomplicated construction.

To improve the reliability of the system it is not possible in this case to arrange parts with redundancy since this would complicate the whole system even more without improving it. It may even be impossible to arrange double parts because no additional space would be available. The only possible suggestion regarding the results of the analysis is to shorten the test frequency for parts with high failure rates, such as brakes, centrifugal friction regulators and gears.

If such components could be inspected daily instead of weekly the availability of the EDF-2 control rod drive mechanism, for instance, could be improved to 0.9998.

For this daily inspection it would be sufficient to operate the drive system for a short rod movement.

3.3. Comparison of Estimated and Operationally Determined Control Rod Drive System Failure Rates

Only sparse information is available on the operational reliability of control rod drive actuators in gas-cooled reactors.

The following values were obtained from a publication (Ref. 5) on the operational reliability of the AEA magnox reactors (Calder Hall and Chapel Cross) for the five-year period 1961-65, which was unaffected by early commissioning and teething trouble. From the distribution of faults in relation to plant areas it was possible to calculate the:

- total control rod system fault occurrences:
  as $3.08 \ 10^{-6} \ \frac{\text{faults}}{\text{system . h}}$

- control rod system fault occurrences causing interruption of operation:
  as $0.59 \ 10^{-6} \ \frac{\text{faults}}{\text{system . h}}$

- total control rod system fault occurrences related to human errors:
  as $0.59 \ 10^{-6} \ \frac{\text{faults}}{\text{system . h}}$
  (the human error faults amount to approximately 10% of the total fault occurrences; 43% of the human error faults were responsible for interruption of reactor operation).

Another article (Ref. 6) gives information on the performance of the Berkeley, Bradwell and Hunterston nuclear power stations for two or one year's (Hunterston) operation. These stations belong to the same generation as the Latina installation. In this article details of plant equipment operation are considered, this relating mainly to turbines.

boilers and reactor fuelling. As far as the control rod systems are concerned, it is stated that the systems have proved entirely satisfactory and flexible. Actuator inspections led to the suggestion that this good performance might continue. From Hunterston's first year of operation it was reported that teething troubles with the control rod system have been experienced but that thereafter the sytem was performing well and no difficulties were envisaged. From the information given in the article no quantitative figures for control rod drive sytem reliability could be evaluated, but qualitatively one gets the impression that control rod drive system availability should be high and possibly even higher than that evaluated for the Calder Hall and Chapel Cross reactors.
More recent information follows from table 4.
The figure given for the total control rod system fault occurrences of the eight Calder Hall and Chapel Cross reactors of $3.08\ 10^{-6}$ $\frac{\text{faults}}{\text{system}}$ are based on 1920 system-years of operational experience.

This figure compares very well with a value evaluated for water cooled power reactors (Dresden 1, Humbold Bay, Indian Point, Shippingport and Yankee) of $1.4\ 10^{-6}$ failures per h of control rod operation (Ref. 7). This value is based on 775 control rod years of operation.

No quantitative operational experience was available for the control rod drive systems of the KDF gas-cooled reactors.

Operational experience with the Latina nuclear power station was, however, available so that failure rates for the control rod drive system could be evaluated. Plant operating data for 1967-68 were considered, e.g., for the fifth year of operation, which should be free of teething troubles, the following values being found (Ref. 12):

- total control rod system fault occurrences

as 19.4 10^{-6} $\frac{\text{faults}}{\text{system.h}}$

(17 occurrences, 100 control rod drives per reactor)

- control rod system fault occurrences causing reactor shut-down (35% of the total occurrences)

as 6.85 10^{-6} $\frac{\text{faults}}{\text{system.h}}$

Most of the total number of defects, e.g., 76.4% (representing 14.8 10^{-6} $\frac{\text{faults}}{\text{system.h}}$) relate to the electrical part of the system; only 23.6% (representing 4.6 10^{-6} $\frac{\text{faults}}{\text{system.h}}$) are due to defects with mechanical parts.

The failure rates estimated for the Latina reactor control rod drives are very useful for a comparison with the analytically determined ones. As was stated before, the analytical analysis performed only takes the mechanical components into account. A failure rate of 8.64 10^{-6} estimated for the Latina drive system must be compared with 4.6 10^{-6} obtained for mechanical faults from operational experience. It must be stated that both values correspond very well, considering that the failure rates of most of the 16 components of the drive system could have been estimated only with a high margin of uncertainty.

It can be concluded that an analytical approach to control rod drive system reliability is possible, as was shown last year too for water-cooled power reactors (Ref. 1). To improve the accuracy of calculated reliability figures, failure rates for all components used in a system must be available.

Collection and treatment of nuclear power plant part and system defect situations in a data bank is essential in order to be able to find the component failure rates needed for such an estimation of reliability.

(Table 5 gives a summary of experimentally determined mechanical failure rate.

3.4. Reliability Analysis for the Entire Control Rod System

Until now the reliability of one single control rod mechanism only has been considered. In a gas-cooled reactor approximately a hundred control rods with their drive mechanisms are arranged in parallel, leading to a redundant system with increased reliability. But only a few units are allowed to fail, so that safe reactor control is possible and shut-down capacity is always available.

The reliability of an entire system for the most important scram case of operation and r stuck rods permitted can be estimated using Poisson's law (Ref. 1):

$$R = \sum_{i=0}^{r} \frac{\left(\frac{t}{\Theta}\right)^{i} \left(e^{-\frac{t}{\Theta}}\right)}{i!}$$

For the three control rod drive mechanisms considered, a scram function reliability analysis has been performed for a complete system using analytically determined failure rates λ_s which differ only slightly from the ones valid for normal operation λ_N (see Table 2) because most of the unit components are involved in scram operation also. The corresponding mean time between failures determined by

$$\Theta_s = \frac{1}{\lambda_s}$$

needed for the reliability evaluation with Poisson's law are listed also.

	KDF-2	KDF-3	Latina
$10^6 \lambda_s \left(\frac{\text{faults}}{\text{system.h}}\right)$	19.10	13.09	8.34
Θ (weeks)	312	455	713

The calculation of system reliability was performed for two more failure rates and mean times between failures

e.g. $\lambda_s = 3 \quad 10^{-6}$ and $0.6 \quad 10^{-6}$ $\left(\frac{\text{faults}}{\text{system.h}}\right)$

$\Theta = 2000$ and 10,000 (weeks),

which represent data obtained from British magnox reactor experience for total fault occurrences and for fault occurrences causing interruption of operation. The calculations are performed for no, one and two stuck rods permitted.

The results of the reliability calculations are listed in Table 3 and plotted in Figs. 20-22.

Fig. 20 indicates total system reliability for the estimated failure rate of the EDF-2 control rod drive unit. System reliability decreases with operating time but only if no stuck rod is permitted for the scram case. The decrease in reliability is small for one stuck rod permitted and approximately zero for two stuck rods permitted.

Fig. 21 shows system reliability for the estimated failure rates of the three control rod drive mechanisms considered dependently of the length of uninspected operating time τ.

A system reliability greater than 0.9990 is obtainable for all three control rod drive types for an uninspected operating time of less than 12 weeks.

In Fig. 22 system reliability is presented versus mean time between failures Θ or failure rate λ, uninspected operating time t and number of stuck rods permitted r. System reliability increases when the uninspected operating time is smaller but mainly when one stuck rod (r = 1) is permitted. The system reliability is then approximately equal to unity for one week and also for six weeks of uninspected operating time for failure rates of between 3 10^{-6} and 20 10^{-6} range of possible values estimated both by analysis and on the basis of operational experience with control rod systems in gas-cooled reactors. System reliability decreases for a longer uninspected operating time t and one stuck rod permitted only if the failure rate is higher than 20 10^{-6} (mean time between failures less than 200 weeks).

It can be concluded that a high (almost 100%) reliability of an entire control rod system can be expected; nuclear reactor design normally allows one stuck rod and reactor operational experience shows that failure rates smaller than 20 10^{-6} are attainable. Furthermore, the untested operating time of a drive unit will be less than six weeks. It can be assumed that the individual control rod is exercised in a one or two week cycle, so that any tendency to stick can be recognized early on.

References

1. J. Ehrentreich, H. Maurer:
Reliability Considerations for Electro-Mechanical and Hydraulic Control Rod Drive Systems
Commission of the European Communities, Doc. 7331/XII/68-E

2. J. Ehrentreich, M. Pantleon:
Die europäische Atomindustrie und ihr Markt - 6. Steuerstäbe und Antriebe für Kernreaktoren
Atomwirtschaft, März 1969, 138-142

3. Electricité de France
Centrales Nucléaires de Chinon EDF-2, EDF-3
Reactor-Descriptions

4. SIMEA
Latina Power Station - Safety Report

5. R. Parker:
The operational reliability of AEA magnox reactors
Journal of the British Nuclear Energy Society, April 1967 Vol.5,N°2

6. D.T. Evans, F.R.R. Jones, W.J. Prior:
The performance of nuclear power station plant
Journal of the British Nuclear Energy Society, July 1965, Vol.4,N°3

7. H.P. Pomrehn:
Power Reactor Control-Rod System Operating Experience
Combustion, March 1967, 8-13

8. A.R. Eames:
Reliability Assessment of Protective Systems
Nuclear Engineering, March 1966, 188-192

9. B.J. Garrick et al
Reliability Analysis of Nuclear Power Plant Protective Systems
May 1967, HN 190

10. Several EUR-Reports of Latina Nuclear Power Plant Operation 1967/68

11. Operating experience - detailed outage analysis from the nuclear power stations operating in the U.K. Nuclear Engineering International vol. 14 (1969) No. 160, 737-740 (September).

Table 1

Estimated Failure Rates of Drive System Components

	Component (see Figs. 8,15,19)	Failure Rate Failures per million h
EDF-2	flange or plug EDF-3 with joint	0.02
	pneumatic cylinder and piston	0.004
	oil regulator	0.008
	rack (see item 1 of EDF-2 system)	2.0
	planetary gear	0.05
	drum type brake	3.0
	shaft	0.1
	centrifugal friction regulator	3.0
	bevel gear and shaft	2.0
	rotary gas seal	0.7
	cable drum	0.5
	cable	0.1
	cable guides and slack cable device	1.0
	cable connecting link	0.5
	control rod wing coupling	0.1
	shock absorber	0.2
	control rod channel	0.02
EDF-3	asynchrone or synchronous (Latina) -motor	0.3
	electrical brake	0.1
	speed limit device (corresponding to centrifugal friction regulator)	3.0
	reduction gear frain	2.0
LATINA	pressure casing	0.02
	eddy current brake	0.1
	winding gear	2.0
	spring loaded pulley	1.2
	control rod shock absorber assembly	0.5

(Ref. 8, 9)

Table 2

Results of the Analytical Analysis of Drive System Reliability

System	Normal operation by weekly inspections			Normal operation by quarterly inspection cycles		
	Failure Rate λ in 10^{-6} operational hrs	Down-time $\lambda\tau$ (τ = 84 h) h	Availability $A = 1 - \lambda\tau$	Failure Rate λ	Down-time $\lambda\tau$ (τ = 1008 h)	Availability $A = 1 - \lambda\tau$
[illegible]-2	19.10	1604	0.99840	19.10	19253	0.98075
[illegible]-3	18.39	1545	0.99846	18.39	18537	0.98146
LAVINA	8.64	726	0.99927	8.64	8708	0.99129

Table 1

Control Rod System Scram Reliability R
calculated by the Poisson Distribution Law
for mean time between failures $\mathcal{O}_s$ and r stuck rods permissible

t (weeks)	R(r=0)	R(r=1)	R(r=2)
a) $\mathcal{O}_s$ = 312 weeks (λ_s = 19.1 . 10^{-6})			
1	0.9968	1.0000	1.0
4	0.9873	0.9999	1.0
6	0.9810	0.9998	1.0
12	0.9622	0.9992	0.9999
16	0.9500	0.9987	0.9999
24	0.9260	0.9972	0.9999
b) $\mathcal{O}_s$ = 455 weeks (λ_s = 13.09 . 10^{-6})			
1	0.9978	1.0	1.0
4	0.9912	0.9999	1.0
6	0.9869	0.9999	1.0
12	0.9740	0.9997	1.0
16	0.9654	0.9994	1.0
24	0.9486	0.9986	0.9999
c) $\mathcal{O}_s$ = 713 weeks (λ_s = 8.34 . 10^{-6})			
1	0.9986	1.0	1.0
4	0.9944	1.0	1.0
6	0.9916	0.9999	1.0
12	0.9833	0.9998	1.0
16	0.9778	0.9997	1.0
24	0.9670	0.9995	1.0
d) $\mathcal{O}_s$ = 2000 weeks (λ_s = 3 . 10^{-6})			
1	0.9995	1.0	1.0
4	0.9980	1.0	1.0
6	0.9970	1.0	1.0
12	0.9940	1.0	1.0
16	0.9920	0.9999	1.0
24	0.9881	0.9999	1.0
e) $\mathcal{O}_s$ = 10000 weeks (λ_s = 0.6 . 10^{-6})			
1	0.9999	1.0	1.0
4	0.9996	1.0	1.0
6	0.9994	1.0	1.0
12	0.9988	1.0	1.0
16	0.9984	1.0	1.0
24	0.9976	1.0	1.0

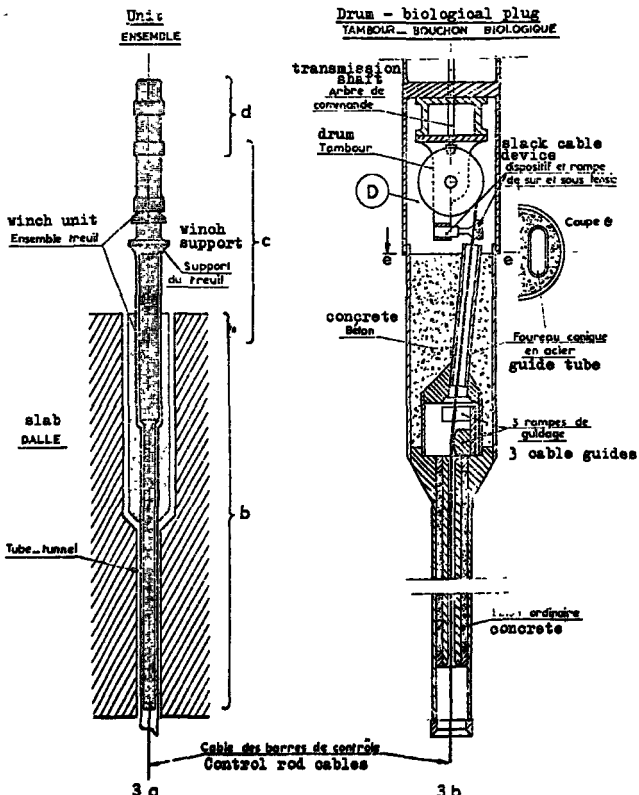


Fig. 1 : EDF-2 Reactor Control Rod Drive Mechanism (pneumatic/mechanical system)

TABLE 4

Control Rod System Fault Occurences and corresponding

Failure Rates responsible for forced Outages of UK Reactor Stations

Station	Operational Period	Reactor Years	No of outages per control rod syst.	Number of control rods per reactor	control rod system failure rate (fault/system.h)
Berkeley	1963 - 68	12	4	132	$0.29 \cdot 10^{-6}$
Bradwell	1963 - 68	12	2	120	$0.15 \cdot 10^{-6}$
Hinkley Point A	1965 - 68	7	3	130	$0.38 \cdot 10^{-6}$
Trawsfynydd	1965 - 68	7	6	110	$0.98 \cdot 10^{-6}$
[illegible] A	1966 - 68	5	3	120	$0.57 \cdot 10^{-6}$
[illegible]	1966 - 68	4	3	107	$0.80 \cdot 10^{-6}$
[illegible]	1968	1	0	101	0

[illegible] Operating experience - detailed outage analysis from the nuclear power stations operating in the U.K. Nuclear Engineering International vol. 14 (1969) No 160, 737-740 (September)

TABLE 5

CONTROL ROD SYSTEM FAULT OCCURENCES (FAULTS/SYSTEM h)

DERIVED FROM OPERATING EXPERIENCE WITH GAS AND WATER COOLED REACTORS

STATION	TOTAL OCCURENCES	OCCURENCES RESPONSIBLE FOR INTERRUPTION OF OPERATION	OCCURENCES RELATED TO HUMAN ERRORS (% OF TOTAL)
UK-GCR			
Calder Hall Chapel Cross	3.08 10^{-6} (1920 system years of operation)	0.59 10^{-6}	0.59 10^{-6}
Latina (in Italy)	19.4 10^{-6} (electr.p. 14.8 10^{-6}, mech.p. 4.6 10^{-6}, mech.calc. 8.6 10^{-6})	6.85 10^{-6}	
Berkeley		0.29 10^{-6}	
Bradwell		0.15 10^{-6}	
Hinkley Point A		0.38 10^{-6}	
Trawsfynydd		0.98 10^{-6}	
Dungeness A		0.57 10^{-6}	
Sizewell		0.80 10^{-6}	
Oldbury		0	
US-WCR			
Dresden 1 Humbold Bay Indian Point Shippingport Yankee	1.4 10^{-6} (775 system years of operation)		

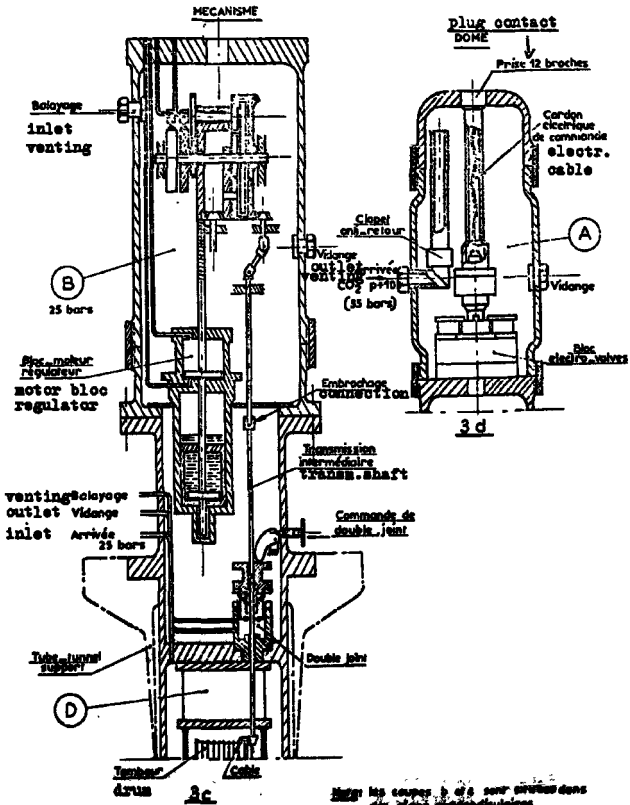
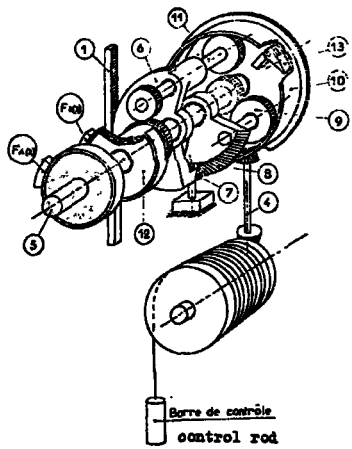
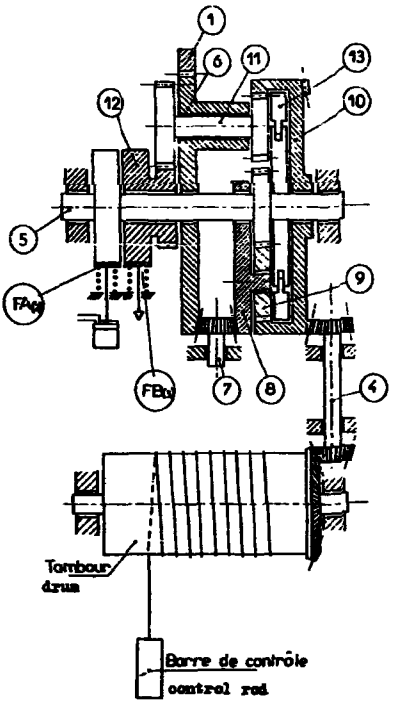


Fig. 2 : KNK-2 Reactor Control Rod Drive Mechanism (details)



1 - Rack
2 - Brake A
3 - Brake B
4 - Intermediate gearing
5 - Shaft
6 - Sector
7 - Conical pinion
8 - Sector
9 - Satellite pinion
10 - Gear rim
11 - Shaft
12 - Brake pulley
13 - Centrifugal friction regulator

Fig. 1 : KDF-2 Reactor Control Rod Drive Mechanism - Perspective View of Gear and Drum System.



1 - Rack
2 - Brake A
3 - Brake B
4 - Intermediate gearing
5 - Shaft
6 - Sector
7 - Conical pinion
8 - Sector
9 - Satellite pinion
10 - Gear rim
11 - Shaft
12 - Brake pulley
13 - Centrifugal-friction regulator

Fig. 4 : BR-2 Reactor Control Rod Drive Mechanism - Gear and Drum System.

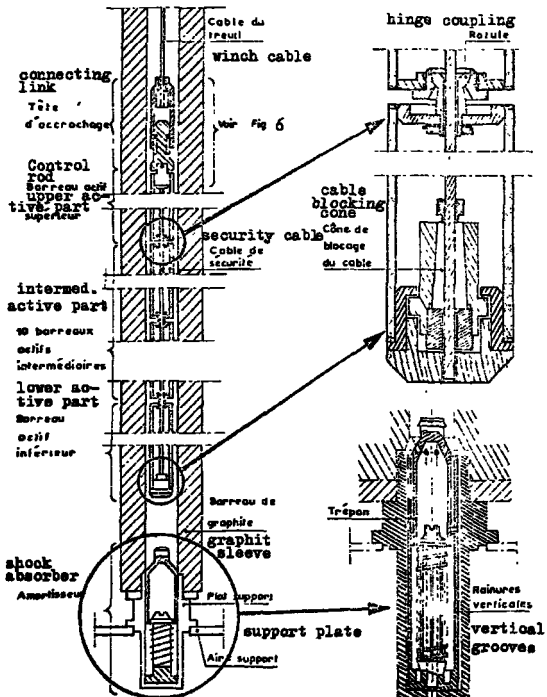


Fig. 5 : EDF-2 Reactor Control Rod - Details.

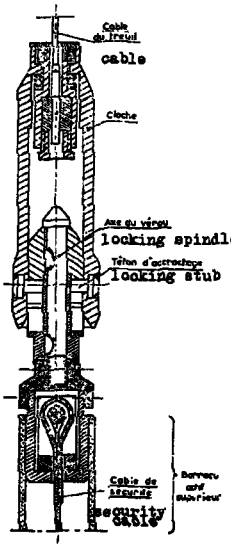
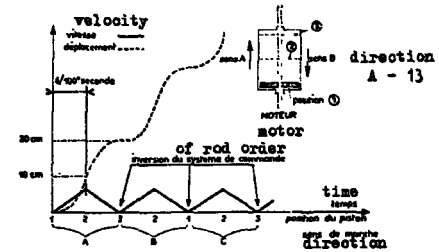
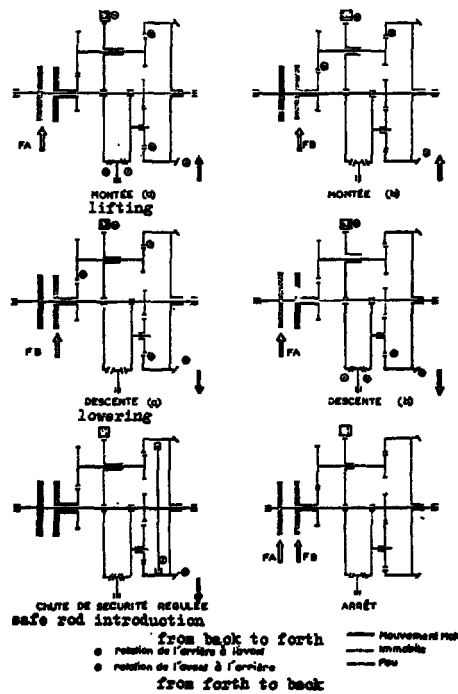


Fig. 6 : KNK-2 Reactor Control Rod - Cable Rod Connecting Link.



Déplacements de la barre
rod deplacement



Mécanisme : Ensemble coupe

Fig. 7 : KNK-2 Reactor Control Rod Drive System - Operational Scheme

Failure rates per 10^6 hours :	components :
0.020	flanges with joint
0.004 0.008	pneumatic cylinder and piston; oil regulator
2.0	rack (item 1)
0.05	planetary gear (items 6,7,8,9,10,11,12)
3.0	drum type brake FB (item 3)
0.1	shaft (item 5)
3.0	drum type brake FA (item 2)
1.0	centrifugal friction regulator (item 13) (driven by satellite pinion (item 9))
2.0 + 2.0	worm, gears and shafts (item 4)
0.7	rotary joint coil
2 x 0.5	cable loops
0.4	cable
2 x 0.1	cable guides and slack cable device
0.5	cable connecting link
12 x 0.1	control rod (12 active parts) with finger couplings
0.1	safety cable (inserted in hinge mountings)
0.2	[illegible]
0.02	[illegible]

Fig. 2 (cont'd)

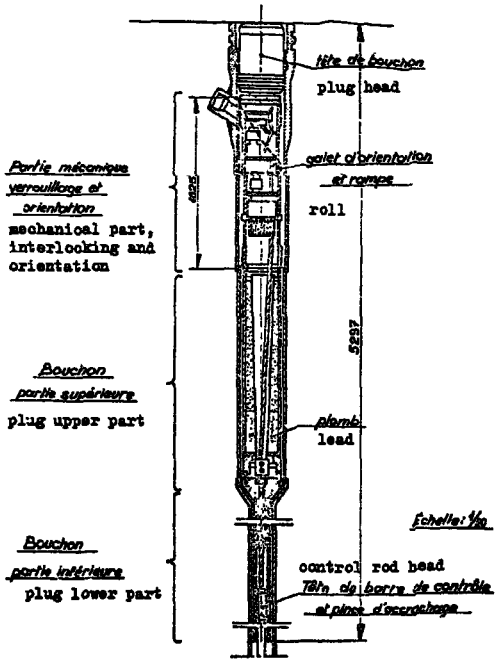
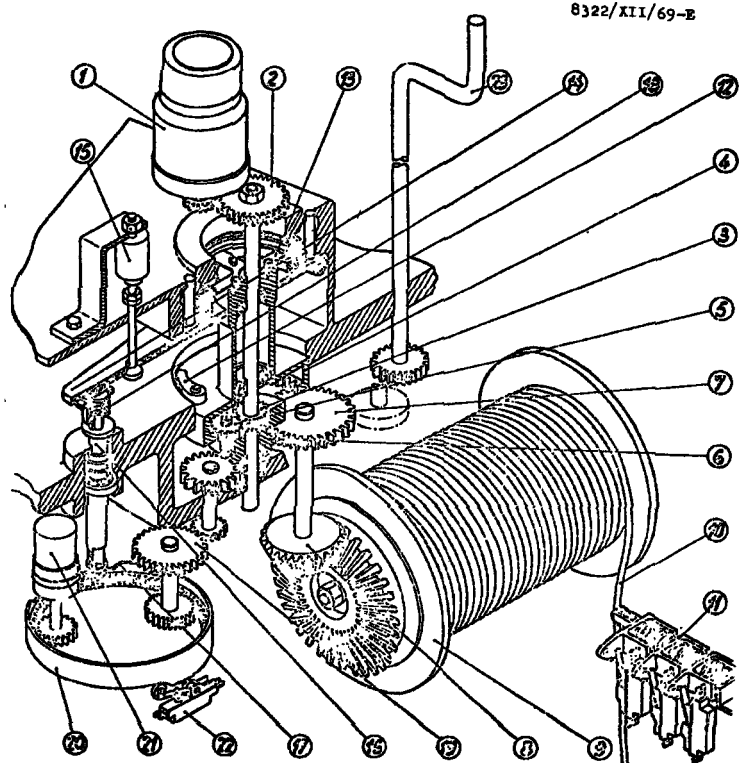


Fig. 9 : REP-3 Reactor Control Rod Drive Mechanism

Parts list

1 - Motor and brake
2 - First reduction gear stage
3 - Central pinion of differential
4 - Outer ring gear of differential
5 - Satellite pinion of differential
6 - Satellite pinion carrier
7 - Second reduction gear stage.
8 - Drum bevel gearing
9 - Cable drum
10 - Cable
11 - Jockey pulley device
12 - Speed regulator
13 - Disk brake
14 - Disk brake lever
15 - Electromagnet for disk brake operation
16 - Rod for mechanical brake operation
17 - Cam for mechanical brake operation
18 - Progressive brake spring
19 - Pinion of the position reproduction device
20 - Outer ring gear of position
21 - Voltage
22 - Limit switch of position indicator
23 - Hand operation

Control Rod Drive Mecha-
Perspective Drawing of Motor,



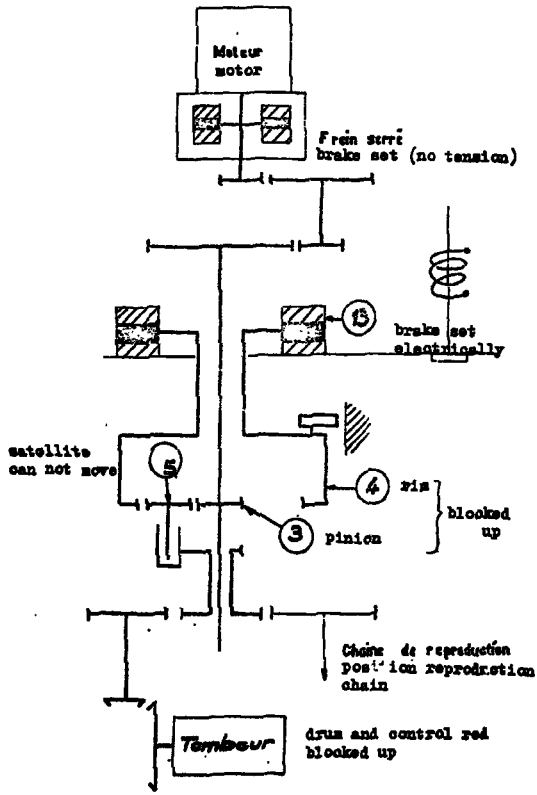


Fig. 11 : Operation of RBMK-3 Reactor Control Rod Drive Mechanism : Rod Stop Period.

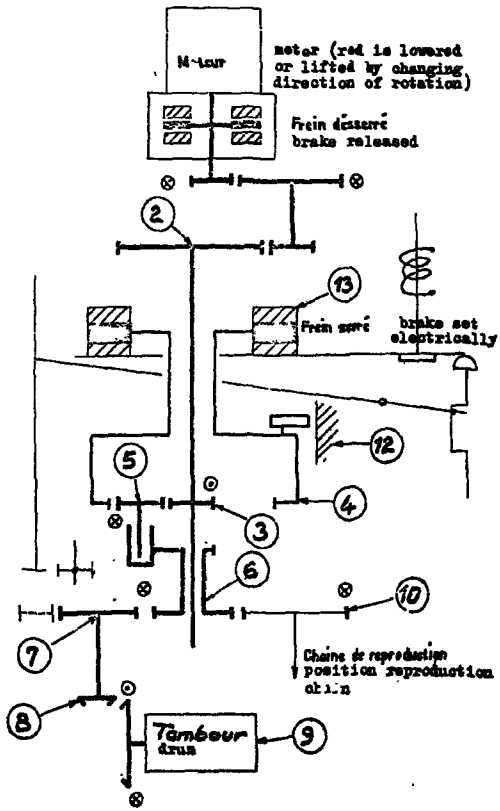


Fig. 12 : Operation of EBWR Reactor Control Rod Drive Mechanism : Normal Operation Period.

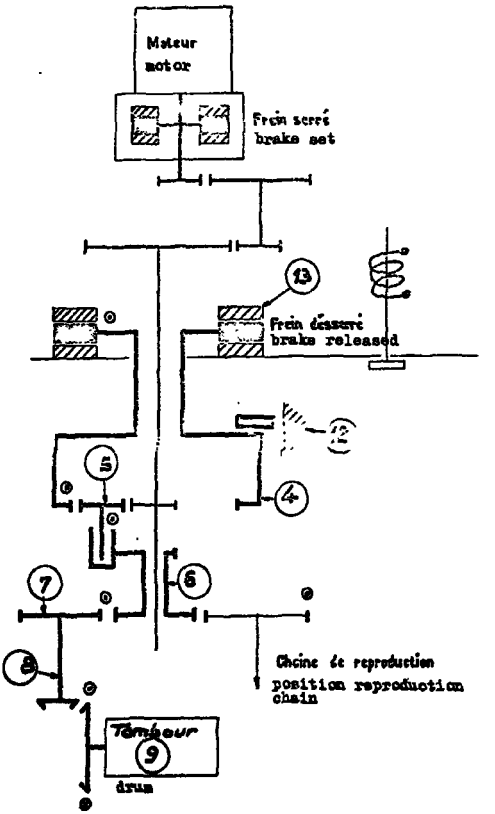
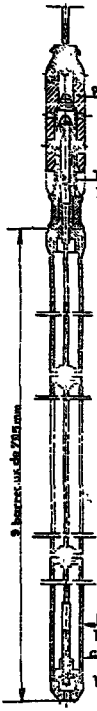
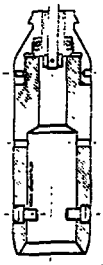


Fig. 13 : Operation of RDF-3 Reactor Control Rod Drive Mechanism : Controlled Rod Drop (Security Chain).



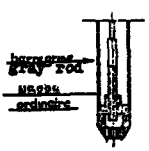
Tête de barre de contrôle.

control rod head



control rod connecting piece

Chapeau d'accrochage de barre de contrôle.



Barre de contrôle avec tête d'accrochage.

control rod with head link

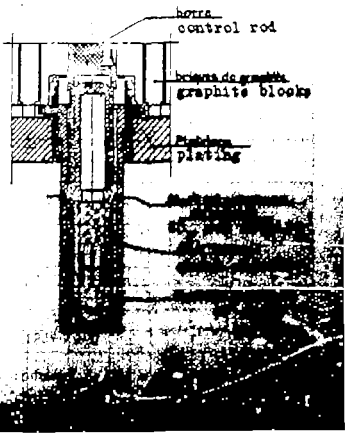


Fig. 14 : EDF-3 Reactor Control Rod — Details.

Calibre nominal DN/mm	Epaisseur e mm
6 000	
	0,3
	0,1
	3,0
	0,5
	0,25
	1,0
	3,0
	2,5 - 3,0
	2 x 0,5
	0,1
	2 x 0,1
	0,5
	2 x 0,5
	0,1
	0,2
	0,25

Fig. 12 / Fig. 12 Exemple d'utilisation / Example of use / Esempio di impiego / Voorbeeld van toepassing

- Commande à piston / piston valve control
- Appareillage-valve
- Actionneur linéaire / linear actuator (item 1)
- Ressort d'appui / spring
- Capteur de pleine course (item 2) / end-of-travel sensor (item 2)
- Flasque / flange (item 3)
- Tige / piston rod (item 4)
- Soufflet / bellows (item 5)
- Corps / body (item 6)
- Siège / seat (item 7)
- Obturateur / closure member (item 8)
- Joint d'étanchéité / sealing (item 9)
- Joint de tige / gland packing (item 10)
- Entretoise / spacer (item 11)
- Chapeau / bonnet (item 12)
- Vis de fixation / fixing screw (item 13)
- Ecrou / nut (item 14)
- Goupille / pin (item 15)
- Rondelle / washer (item 16)
- Ecrou de blocage / locknut (item 17)
- Ecrou de réglage / adjusting nut (item 18)
- Contre-écrou / locknut (item 19)
- Vis de réglage / adjusting screw (item 20)
- Vis de blocage / locking screw (item 21)
- Vis de fixation / fixing screw (item 22)
- Vis de fixation / fixing screw (item 23)
- Vis de fixation / fixing screw (item 24)
- Vis de fixation / fixing screw (item

REF	DESCRIPTION
1	MOTOR TERMINAL BLOCK — 4 WAY
2	AUXILIARY TERMINAL BLOCK — 7 WAY
3	ADJUSTABLE BRAKE MAGNET
4	ASSY OF EDDY CURRENT BRAKE
5	PRESSURE CASING
6	ASSY OF MOTOR
7	ASSY OF PULE WHEEL MECHANISM
8	ASSY OF WORM GEAR
9	CHAIN DRUM
10	MAGSLIP TRANSMITTER
11	SLACK CHAIN INDICATOR MICROSWITCH
12	MAGSLIP DRIVE GEARING
13	HAND WINDING MECHANISM
14	LOCKING BRACKET

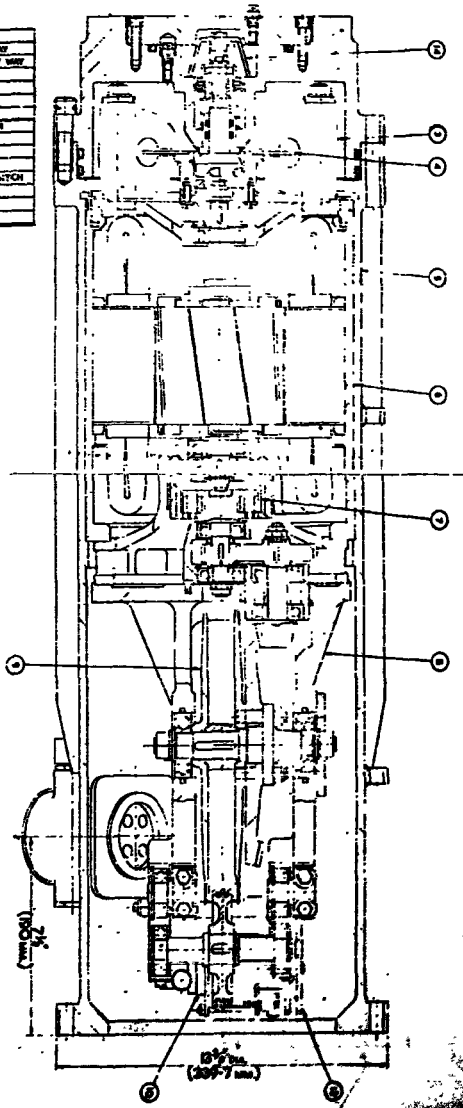


Fig. 16 : LATINA

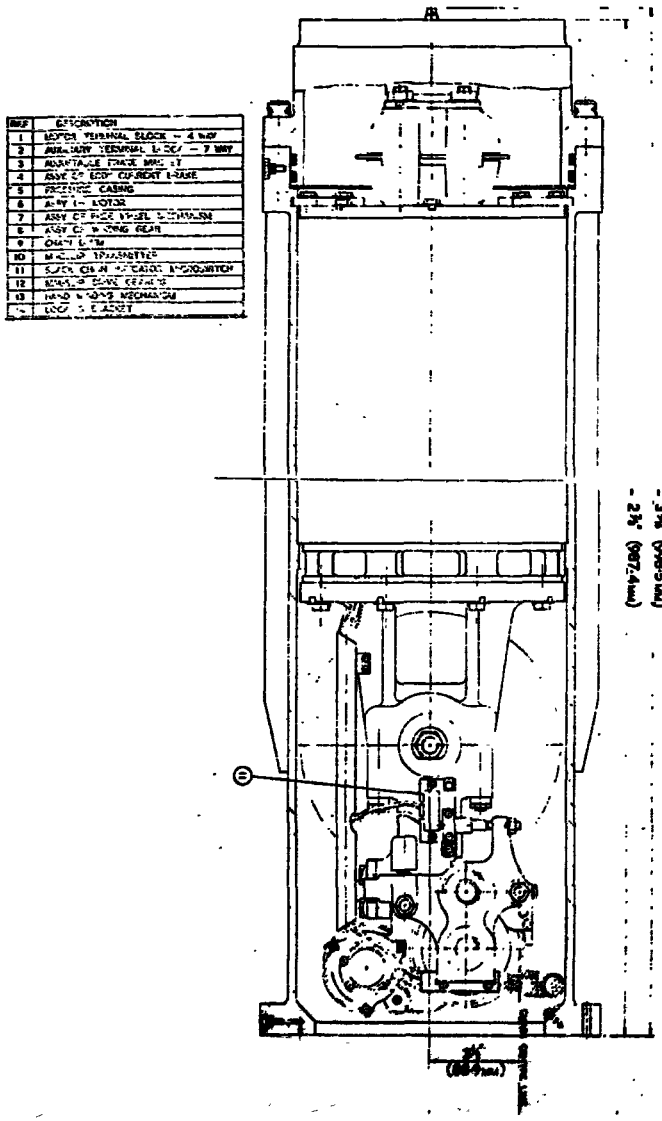


Fig. 11. [illegible] BOMBER REQ. ACTUATOR

Ref No.	Drawing No.	Qty.	Code No.	Name of Part
1	[illegible]	1	L3494	LIFTING HEAD
2	[illegible]	1	L3495	SLEEVE
3	[illegible]	1	13545	CABLE CONNECTING LINK
4				
5	[illegible]	1	L3496	SEALING FLANGE
6	[illegible]	1	L3497	GUIDING FLANGE
7	[illegible]	1	L3498	BODY TUBE
8	[illegible]	1	L3499	ABSORBER ASSEMBLY INSERTS
9	[illegible]	1	L3500	LOWER TUBE
10	[illegible]	1	L3501	SHOCK ABSORBER CYLINDER
11	[illegible]	1	L3502	SHOCK ABSORBER PISTON UNIT
12	[illegible]	1	L3503	SHOCK ABSORBER PISTON HEAD
13	[illegible]	1	L3504	SHOCK ABSORBING MATERIAL
14	[illegible]	1	L3505	END CAP
15	[illegible]	1	L3506	TIE ROD
16	---	1	---	WASHER FOR REF No 15
17	---	1	---	NUT FOR REF No 15
18				

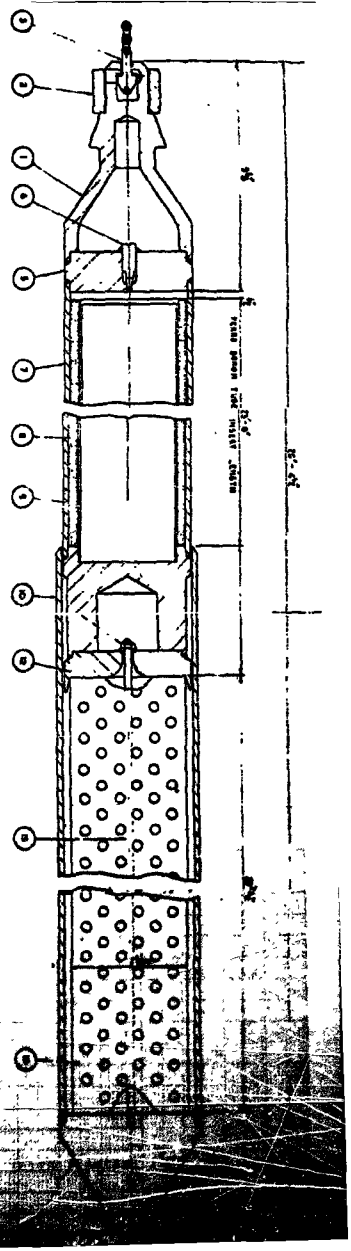


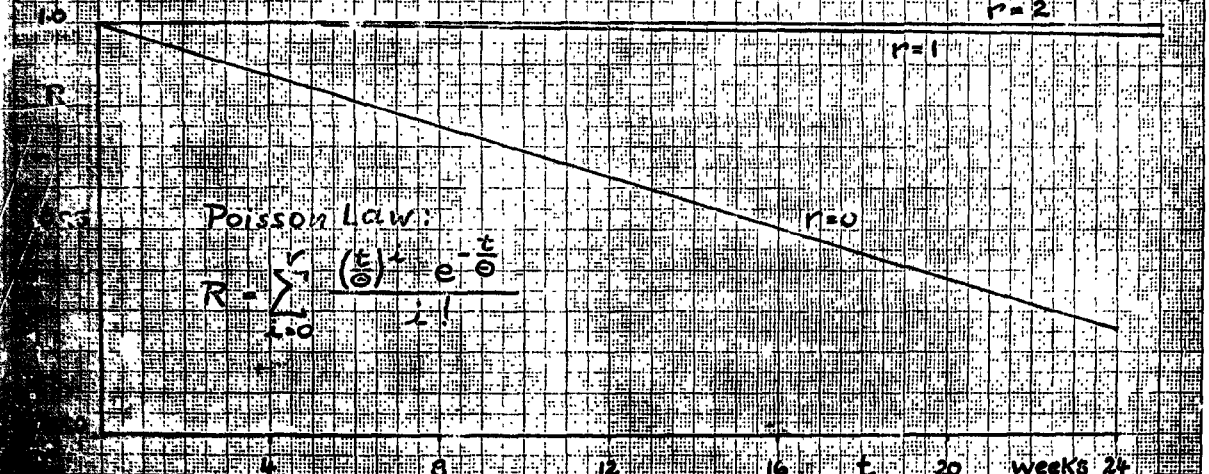
FIG. 18 : Latina Reactor Control Rod

failure rates per 10^6 hours :	components :
0.02	pressure casing (item 5)
0.1	eddy current brake (item 4)
0.3	synchronous motor (item 6)
0.1	motor shaft
0.3	free-wheel mechanism (item 7)
2.0 + 2.0	winding gear (item 8)
2 x 0.5	chain drum (item 9)
1.0 + 0.2	spring loaded pulley
0.1	chain
0.5	chain connecting link
0.5	control rod (active portion)
0.5	control rod shock absorber assembly
0.02	control rod channel

Fig. 19 : Eximus Control Rod Drive Mechanism

$\lambda_s = 19.1\ 10^{-6}$ faults / system · h

$\Theta_s = 312$ weeks



Poisson Law:

$$R = \sum_{i=0}^{r} \frac{\left(\frac{t}{\Theta}\right)^i e^{-\frac{t}{\Theta}}}{i!}$$

Fig. 20 : Control Rod System Reliability R dependent on uninspected operating time t (weeks) for constant mean time between failures Θ (or failure rate λ) and r stuck rods permitted

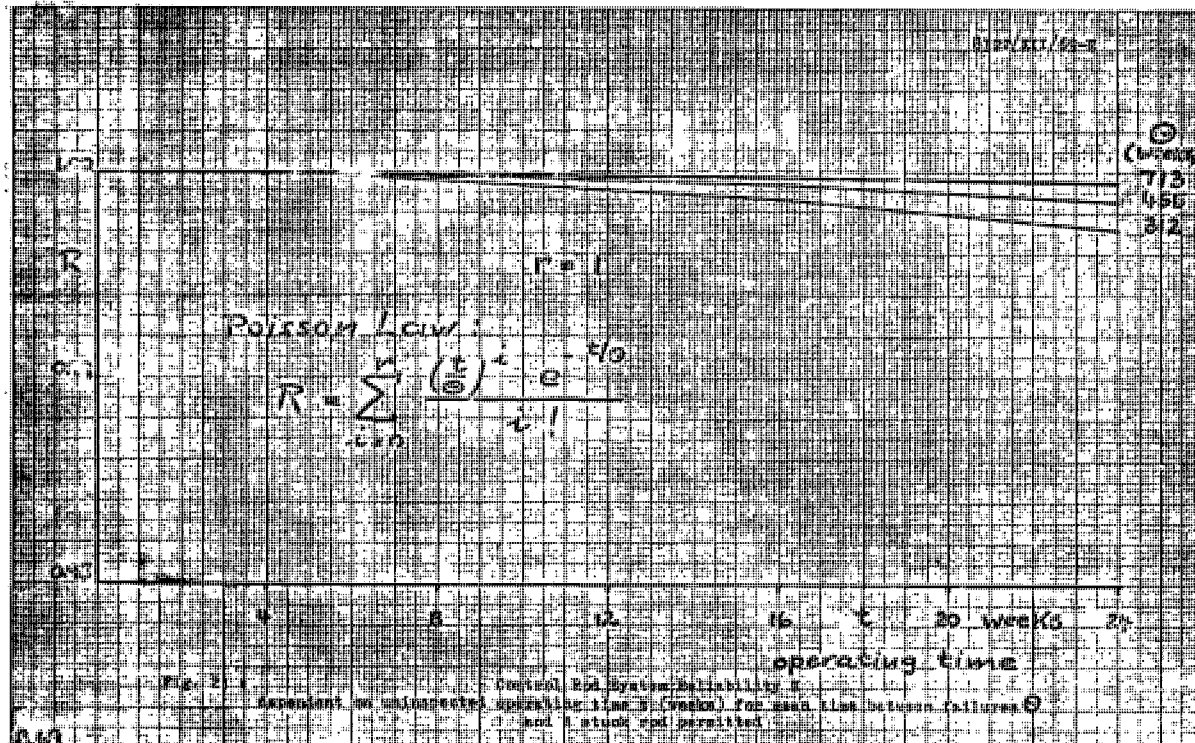


Fig. 2.1 Control Rod System Reliability R

Assessment on subsequent operating time t (weeks) for each risk between failures θ and 4 stuck rod permitted

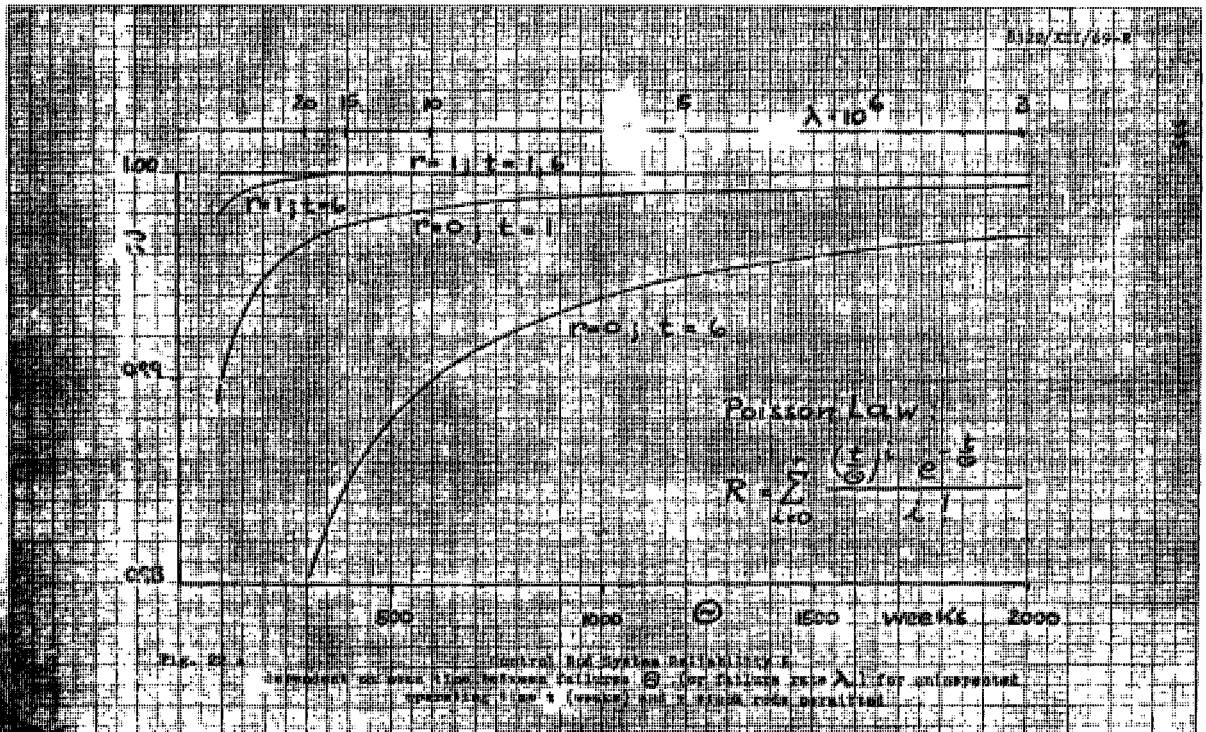


Fig. 12.4 Control R/M System Reliability R
R against mean time between failures θ (or failure rate λ) for uniprocessor system (r = 1 or 3 (voter)) and 3 stage code operations

E.D.F. Juillet 1969

AGENCE EUROPEENNE POUR L'ENERGIE NUCLEAIRE

COMITE DES TECHNIQUES DE SECURITE DES REACTEURS

Réunion de spécialistes en matière de fiabilité des composants et des systèmes mécaniques destinés à assurer la sécurité des réacteurs

QUELQUES MODELES MARKOVIENS DE FIABILITE

par M. CHATELAIN

1.- OBJET

Très généralement une unité de production est formée d'un ensemble de composants (identiques ou non identiques) organisés en un système selon une certaine structure.

Dans les modèles présentés, on détermine sous certaines hypothèses les caractéristiques de fiabilité du système, connaissant

- les caractéristiques de fiabilité des composants
- la structure du système

...

PLAN

3.-

Au-delà de cette technique de prévision, beaucoup de problèmes de fiabilité consistent à déterminer la structure optimale d'un système de composants relativement à un critère donné. Si, par exemple, le critère retenu est celui du coût minimal , on effectuera le bilan économique : coûts d'un perfectionnement de structure d'une part, coûts que ce perfectionnement permet d'éviter d'autre part.

C'est précisément pour apprécier le second terme de ce bilan qu'on doit savoir prévoir les caractéristiques de fiabilité d'un système de composants.

2 - RAPPELS THEORIQUES

2.1. Processus semi-markoviens

2 1 1 Définitions

Un processus semi-markovien (P S.M) est un processus aléatoire qui se déplace d'un état à un autre, ces états étant choisis dans un ensemble dénombrable d'états ; les états successifs visités forment une chaîne de Markov et le processus stationne dans un état donné pendant une durée aléatoire dont la loi dépend de cet état mais aussi du suivant qui sera visité. Ainsi, un P.S.M est une chaîne de Markov pour laquelle l'échelle des temps a été transformée de manière aléatoire.

Plus précisément, la "durée de vie" T de l'état i admet $F_{ij}(t)$ pour fonction de répartition, sachant que l'état suivant sera l'état j ; à la fin d'une durée de vie de l'état i, le choix de l'état suivant est soumis à la matrice de transition $P = ((P_{ij}))$ où P_{ij} est la probabilité du passage de l'état i à l'état j. Le processus est complètement défini si l'on connaît de plus le vecteur A des probabilités initiales de chaque état.

De manière équivalente le processus est défini par la matrice des répartitions de transition Q(t) :

$$Q_{ij}(t) = P_{ij} \quad F_{ij}(t)$$

avec :

$$Q_{ij}(t) = 0 \quad \text{pour} \quad t \leqslant 0$$

$$Q_{ij}(+\infty) = P_{ij}$$

$$\sum_j P_{ij} = 1$$

La matrice $F(t) = ((F_{ij}(t)))$ est alors définie par

$$F_{ij}(t) = P_{ij}^{-1} \; Q_{ij}(t), \quad \text{si} \quad P_{ij} > 0$$

$F_{ij}(t)$ quelconque, si $P_{ij} = 0$

Le P S M est donc défini par le triplet : $(\mathcal{E}, A, Q(t))$

Un processus markovien de renouvellement (P.M.R.) est un processus aléatoire qui recense le nombre de fois $N_i(t)$ où l'on a visité chaque état possible i pendant le temps $[0, t]$ avec l'hypothèse qu'on se déplace d'état en état selon un P S M. Un processus de renouvellement (c'est-à-dire une séquence de variables aléatoires non-négatives, indépendantes et de loi identique) apparaît ainsi comme un P M.R. à un seul état ; la théorie que nous utilisons apparaît comme un mariage de la théorie des chaînes de Markov et de celle du renouvellement. La référence [1] donne tous les détails sur le lien étroit qui lie les P.S.M. et les P.M.R.

En fait, on s'intéressera uniquement au cas où le nombre d'états est fini et dans les deux modèles traités, $Q_{ij}(t)$ sera de la forme :

$$Q_{ij}(t) = P_{ij} \quad \max\,(0, 1 - e^{-\lambda_i t}) \quad (-\infty < t < \infty \,,\, \lambda_i > 0)$$

Il s'agit alors d'un processus markovien en temps continu ou plus simplement continu.

On aura de plus : $P_{ii} = 0, \; \forall \; i$

Mais, on verra que dans certains cas on peut lever l hypothèse de loi exponentielle

L exemple qui suit montrera que la richesse de la théorie des P S M est bien adaptée aux problèmes de fiabilité si l'entretien préventif se borne à un entretien systématique au bout d un temps t_0 de fonctionnement

$$\begin{cases} F_{12}(t) = 0 & \text{si } t < t_0 \\ F_{12}(t) = 1 & \text{si } t \geq t_0 \end{cases}$$

en notant 1 le fonctionnement et 2 l entretien préventif

2 1 2 Principales relations matricielles

Les résultats suivants sont relatifs au cas d'un nombre fini d états

Notons P[A/B] la probabilité de l événement A conditionnée par l événement B

Si Z(t) représente l état dans lequel se trouve le processus à l instant t

$$G_{ij}(t) = P\left[N_j(t) \geq 0 \;/\; Z(0) = i\right] \quad \text{pour} \quad t \geq 0$$

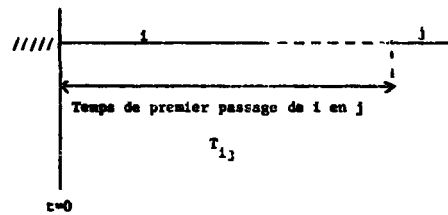
en notant que pour i = j la fonction $G_{ii}(t)$ inclut la probabilité pour que le processus reste dans l état i

De manière équivalente

$$G_{ij}(t) = P\left[T_j \leq t \;/\; Z(0) = i\right] \qquad \text{si} \quad t \geq 0$$

où T_j est l'instant où pour la première fois Z = j

$G_{ij}(t)$ est donc la fonction de répartition du temps T_{ij} de premier passage mesuré de l'instant où le processus entre dans l'état i jusqu'à l'instant où il entre pour la première fois dans l'état j



$$P_{ij}(t) = P[\ Z(t) = j \ / \ Z(0) = i\ ] \quad \text{pour } t \geqslant 0$$

$$N_{ij}(t) = E[N_j(t) \ / \ Z(0) = i]$$

Si l'on note $q^*(s)$, $g^*(s)$, $p^*(s)$, $m^*(s)$ les matrices ayant pour éléments les transformées de Laplace-Stieltjes de Q_{ij}, G_{ij}, P_{ij} et N_{ij}, il est montré à la référence [1] :

$$g^*(s) = q^*(s)[\ I - q^*(s)\ ]^{-1} \qquad \left\{ d\ [\ (I - q^*(s))^{-1}\ ] \right\}^{-1}$$

où dA représente la matrice obtenue à partir de A en remplaçant les éléments en-dehors de la diagonale principale par des zéros

$$p^*(s) = (I - q^*(s))^{-1} \ (I - h^*(s))$$

avec :

$$H_{ii}(t) = \sum_j Q_{ij}(t)$$

$$H_{ij}(t) = 0 \quad \text{si } j \neq i$$

$$m^*(s) = q^*(s)\ [\ I - q^*(s)]^{-1} = [\ I - q^*(s)]^{-1} - I$$

où I est la matrice unité correspondante

Dans le cas particulier d'un processus markovien continu tel que

$$F_{ij}(t) = 1 - e^{-\lambda_{it}} \quad \text{si l'on définit la matrice :}$$

$$\Lambda = ((\delta_{ij}\ \lambda_i^{-1})) \qquad \delta_{ij} = 1 \quad \text{si} \quad i = j$$
$$= 0 \quad \text{si} \quad i \neq j$$

$$q^*(s) = (I + s\Lambda)^{-1} P$$

et les seuls problèmes pratiques deviennent

1°) - d'inverser la matrice $I - (I + s\Lambda)^{-1} P$

2°) - de revenir aux matrices originales sans qu'on soit assuré à notre connaissance que les polynômes en dénominateur des images aient tous leurs zéros réels

2.1.3 Espérances des temps de premier passage

Notant μ_{ij} et ℓ_{ij} les espérances des variables aléatoires ayant respectivement $F_{ij}(t)$ et $G_{ij}(t)$ pour fonctions de répartition, on peut déterminer ℓ_{ij}

Dans le cas positivement régulier (1), il existe un vecteur-ligne $\widehat{\Pi} = (\Pi_i)$ des probabilités limites de la chaîne de Markov associée Il est montré à la référence [2], page 133 et suivantes :

$$\ell_{ii} = \frac{1}{\Pi_i} \sum_K \Pi_K \mu_K \quad \text{avec} \quad \mu_K = \sum_i p_{Ki} \mu_{Ki}$$

On peut également calculer directement la variance correspondante σ^2_{jj}

(1) C'est-à-dire quand il n'existe qu'une seule classe d'états, finale et acyclique.

Pour calculer ℓ_{ij} ($j \neq i$) dans le cas où tous les états "communiquent" on peut modifier P de façon à rendre l'état j absorbant ; notons $\bar{P}$ la matrice de passage des autres états non-absorbants

$$\ell_{ij} = \sum_{K \neq j} m_{iK} \mu_K$$

où $((m_{iK})) = (I - \bar{P})^{-1}$; m_{iK} représente l'espérance du nombre de visites à l'état K avec départ dans l'état i pour la chaîne de Markov associée

2.1.4 Résultats en régime limite (c'est-à-dire quand $t \longrightarrow \infty$)

Pour un processus markovien continu (en fait sous des hypothèse. plus générales, voir [1])

$$P_j^* = \lim_{t \to \infty} P_{ij}(t) = \frac{\mu_j}{\ell_{jj}} = \frac{\widehat{\pi}_j \mu_j}{\sum_K \widehat{\pi}_K \mu_K}$$

si $\ell_{jj} < \infty$ et $\sigma^2_{jj} < \infty$

$$\lim_{t \to \infty} \left(\frac{M_{ij}(t)}{t}\right) = \frac{1}{\ell_{jj}}$$

Le premier membre représente en régime limite, l'espérance du nombre de visites à l'état j par unité de temps

2.2. Processus de vie et de mort (référence [3])

2.2.1 Définition

$P_{ij}(t) = P[\, Z(t) = j \,/\, Z(0) = i \,]$ est telle que, quand $t \longrightarrow 0$ et quelle que soit l'origine du temps,

$$P_{ij}(t) = \begin{cases} a_i\, t + 0(t) & \text{si } j = i+1 \\ b_i\, t + 0(t) & \text{si } j = i-1 \\ 1-(a_i+b_i)t + 0(t) & \text{si } j = i \\ 0(t) & \text{dans les autres cas.} \end{cases}$$

où $0(t)$ est un infiniment petit d'ordre supérieur à t

Un processus de vie et de mort est donc un processus markovien continu particulier où, en utilisant les propriétés classiques de la loi exponentielle :

$$P_{i,\,i+1} = \frac{a_i}{a_i + b_i} \qquad P_{i,\,i-1} = \frac{b_i}{a_i + b_i}$$

(les autres éléments de la matrice P étant nuls) et $\lambda_i = a_i + b_i$

2.2.2. Lois des temps de premier passage

Soit A la matrice :

$$A = \begin{bmatrix} -a_0 & a_0 & 0 & 0 & \cdots & 0 & 0 \\ b_1 & -(a_1+b_1) & a_1 & 0 & \cdots & 0 & 0 \\ 0 & b_2 & -(a_2+b_2) & a_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & & -(a_{N-1}+b_{N-1}) & a_{N-1} \\ 0 & 0 & 0 & 0 & & b_N & -b_N \end{bmatrix}$$

Utilisons la matrice A pour définir un système de polynômes $[Q_K(x)]$ à l'aide desquels s'exprimeront simplement les caractéristiques de fiabilité du système :

$$Q_0(x) = 1$$

$$-x\,Q_0(x) = -a_0\,Q_0(x) + a_0\,Q_1(x)$$

$$-x\,Q_K(x) = b_K\,Q_{K-1}(x) - (a_K + b_K)\,Q_K(x) + a_K\,Q_{K+1}(x)$$

$$0 < K \leqslant N$$

Une représentation intégrale des probabilités de transition $P_{ij}(t)$ en fonction de ces polynômes et d'une mesure discrète par rapport à laquelle les polynômes sont orthogonaux a été obtenue à la référence [3] (1957).

Il est établi à la référence [3] (1959) que :

$$\pi^*_{ij}(s) = \frac{Q_i(-s)}{Q_j(-s)} \quad \text{si } j > i$$

$$= \frac{\bar{Q}_{N-i}(-s)}{\bar{Q}_{N-j}(-s)} \quad \text{si } j < i$$

où $[\bar{Q}_K(s)]$ est le système de polynômes correspondant au même processus mais en renumérotant les états de telle sorte que l'état N devienne l'état zéro, etc ...; les paramètres correspondants valant :

$$\bar{a}_K = b_{N-K} \quad \text{et} \quad \bar{b}_K = a_{N-K}$$

...

Le seul problème à résoudre pour revenir à l'originale $g_{ij}(t)$ est de déterminer les zéros du polynôme en dénominateur pour décomposer $g^*_{ij}(s)$ en éléments simples (1).

2.2.3. Moments des temps de premier passage

La détermination des moments (espérance et variance) du temps T_{ij} est explicite en remarquant que si $j > i$, $T_{ij} = T_{oj} - T_{oi}$.

Notons $E_j = E(T_{oj})$ et $V_j = V(T_{oj})$.

On sait, en revenant à la définition de la transformée de Laplace, que E_j est égale, au signe près, à la valeur prise à l'origine par la dérivée première de $g^*_{oj}(s)$:

$$E_j = - \left[\frac{\partial g^*_{oj}(s)}{\partial s} \right]_{s=0}$$

Différentiant la relation de récurrence définissant les polynômes, faisant $x = 0$ et résolvant par deux sommations successives, on obtient finalement :

$$E_j = \sum_{k=0}^{j-1} \frac{1}{a_k \rho_k} \sum_{r=0}^{k} \rho_r$$

$$V_j = E_j^2 - 2 \sum_{k=0}^{j-1} \frac{1}{a_k \rho_k} \sum_{r=0}^{k} \rho_r E_r$$

(référence [3]), 1959).

...

(1) On montre que ces zéros sont tous réels et positifs, la densité $g_{ij}(t)$ est donc toujours constituée d'une somme d'exponentielles décroissantes.

2.2.4. Probabilités en régime limite

Le processus de Markov étant positivement régulier, notons seulement le résultat intéressant :

$$P_j^* = \lim_{t \to \infty} P_{ij}(t) = \frac{\rho_j}{\rho}$$

avec $\rho_j = \frac{a_0 a_1 \cdots a_{j-1}}{b_1 b_2 \cdots b_j}$ et $\rho = \sum_{j=0}^{N} \rho_j$

$$\rho_0 = 1$$

Ce résultat provient de la relation simple obtenue par récurrence :

$$P_j^* \cdot a_j = P_{j+1}^* \cdot b_{j+1}$$

3 - HYPOTHESES COMMUNES ET CLASSIFICATION DES MODELES

3.1. Hypothèses

Dans les rappels théoriques, nous venons d'utiliser le mot "état" au sens d'"état du processus".

Nous allons maintenant utiliser le mot "état" en un sens très différent, celui d'"état des composants", "état du système" pour caractériser la charge disponible par rapport à la charge nominale (des composants ou du système).

On appelle disponibilité (d'un composant ou du système) le rapport de la quantité produite à la quantité productible à charge nominale.

Dans les applications aux modèles, le sens du mot "état" sera précisé pour éviter toute confusion.

...

3.1.1. Hypothèses sur les composants

1°) Chaque composant ne peut prendre que trois états : le fonctionnement à charge nominale, l'indisponibilité totale, la réserve c'est-à-dire la disponibilité totale sans fonctionnement.

Alors que la durée de réserve dépend de la structure du système, les durées de fonctionnement et d'indisponibilité ne dépendent que du type de composant. Les caractéristiques de fiabilité d'un composant sont exhaustivement les lois de probabilité des durées de fonctionnement et d'indisponibilité.

La durée d'indisponibilité d'un composant s'avère être en effet une grandeur aussi importante que sa durée de fonctionnement.

2°) Les lois des durées seront en général exponentielles, c'est-à-dire que les probabilités à un instant donné de tomber en panne ou de sortir d'indisponibilité seront supposées constantes. Les cas où la théorie générale s'applique avec des lois non exponentielles seront signalés et caractérisés. En particulier, il peut s'avérer réaliste de supposer une probabilité non nulle de tomber en panne au début du fonctionnement.

Au sein d'un même composant, les durées de fonctionnement et d'indisponibilité seront des variables aléatoires indépendantes en probabilité. Les durées relatives à un composant seront de même supposées indépendantes de toutes celles relatives aux autres composants.

3.1.2. Hypothèses sur la structure

1°) Il faut d'abord connaître les composants dont est constitué le système : types, nombres de chaque type. Soit N le nombre total de composants

2°) Il faut ensuite connaître les règles de gestion du système c'est-à-dire comment se modifient les états de tous les composants quand un composant tombe en panne ou redevient disponible.

...

Pour préciser ces règles, représentons le système à l'aide de deux "services".:

- un service D ne comprenant que des composants disponibles formé lui-même de deux services :

  . un service F de composants en fonctionnement

  . un service S de composants en stock (on dira aussi en réserve).

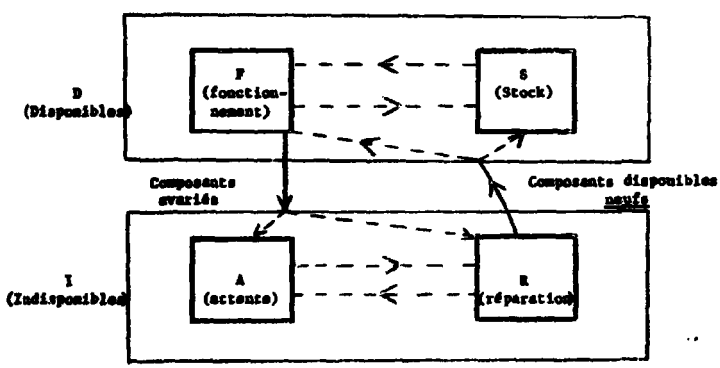
Les composants qui sortent du service D sont considérés comme avariés.

- un service I ne comprenant que des composants indisponibles formé lui-même de deux services :

  . un service R où les composants sont réparés ou remplacés

  . un service A où les composants avariés attendent.

Les composants qui sortent du service I sont considérés comme neufs, c'est-à-dire qu'ils ont mêmes lois de durée de fonctionnement qu'au début quel que soit le nombre de passages en R.



Les flèches symbolisent les possibilités de passage d'un composant d'un service à un autre ; ces passages sont supposés instantanés En ce sens on dira que les composants dans S sont en réserve installée.

Les flèches en trait plein symbolisent les possibilités de passages qui ne dépendent que du composant (ou plutôt de son type) : à un instant donné un composant a une certaine probabilité de devenir indisponible s'il est en F et une certaine probabilité de devenir disponible s'il est en R. Ce type de passage d'un composant entre D et I sera appelé un saut.

On a fait les hypothèses réalistes suivantes

- aucun saut n'est possible à partir de A et de S, autrement dit :

  . un composant ne se répare pas en attendant

  . un composant en réserve ne tombe pas en panne sans passer au préalable par F même s'il y reste un temps très court (voir les hypothèses sur les lois des durées).

- à un instant donné, il se produit un saut au plus (la probabilité de deux sauts ou plus est au moins du second ordre).

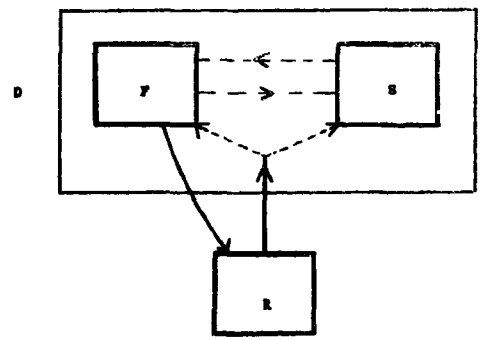
- les sauts commandent les autres passages, c'est-à-dire que tous les instants de passage sont des instants de saut.

Les flèches en trait pointillé symbolisent les possibilités de passage qui se produisent au moment des sauts et sont déterminées par les règles de gestion :

—▶ concernant le service I les règles de gestion se résument en une seule : le service A est toujours vide, c'est-à-dire que l'on suppose que R a une "capacité" suffisante pour répondre à toutes les demandes. La nécessité de cette hypothèse vient du fait qu'il est difficile d'analyser la grande diversité des situations correspondant à l'immobilisation d'un matériel (voir le paragraphe 4.2 1). Les paramètres des lois de durée d'indisponibilité devront être déterminés en tenant compte de cette hypothèse fondamentale en "intégrant" la dispersion des durées : il suffit pour cela d'observer les durées réelles d'indisponibilité par composant.

...

Les modèles présentés auront donc le schéma suivant en commun où les trois "services" F, R et S symbolisent les trois états possibles des composants : fonctionnement, indisponibilité et réserve



⟶ concernant le service D les règles de gestion dépendant du modèle.

3°) Enfin l'état du système ne dépend que des états des composants par l'intermédiaire de la fonction de structure f. Cette fonction est certaine.

Si x_i représente l'état du composant (i) $f(x_1, x_2, \ldots, x_n)$ représente l'état du système.

Les états du système seront caractérisés dans chaque modèle par la charge disponible du système comprise entre zéro et la charge nominale. A l'inverse des composants le système peut prendre un ou des états à charge réduite.

Un ensemble de coordonnées $(x_1, x_2, \ldots, x_n)$ sera naturellement appelé un point. Un point caractérise une configuration des états des composants du système et la fonction de structure est une fonction de points. En raison de l'existence des règles de gestion, il n'est généralement pas possible d'atteindre tous les points.

3.2. But recherché

On a défini ce qu'on entendait par caractéristiques de fiabilité d'un composant. De même les caractéristiques de fiabilité du système sont les lois des durées des états du système et les probabilités de passage d'un état à un autre quand le système peut prendre plus de deux états.

Ce sont ces lois et ces probabilités qu'on s'efforcera de déterminer sous les hypothèses les plus générales en sachant bien que cette formulation suppose qu'un système de composants à comportement markovien, a lui-même un comportement markovien, ce qui n'est pas le cas en général (voir § 4.2.4. et 5.4.).

3.3. Classification des modèles

3.3.1. Définition de l'identité de deux composants

Deux composants sont réputés identiques (ou de même type) si les trois conditions suivantes sont réalisées :

- ils ont même loi des durées de fonctionnement et même loi des durées d'indisponibilité et en particulier mêmes valeurs des paramètres,

- la fonction de structure et donc l'état du système ne sont pas modifiés, quand un des composants prend l'état de l'autre (et vice-versa) quels que soient ces états.

Si, dans le cas de deux composants, $f(x_1, x_2)$ est la fonction de structure du système, la seconde condition s'écrit :

$$f(x_1, x_2) = f(x_2, x_1) \quad \forall\ x_1, \forall\ x_2$$

- ils ont mêmes règles de gestion.

...

3 3 2 Premier type de modèle composants identiques

L'état du système ne dépend alors que du nombre (ou des nombres) de composants dans tel ou tel état Dans le modèle présenté la fonction de structure ne dépendra que du nombre de composants indisponibles, c'est-à-dire du nombre de composants dans le service R

Ce modèle classique recouvre une partie des problèmes parfois connus sous le nom "Problèmes du réparateur" ([2] pages 139 et suivantes) et se rattache aux modèles de files d attente puisque tous les "clients" sont identiques

Lorsque toutes les lois des durées sont exponentielles, on a affaire à un processus de vie et de mort

Lorsque les lois des durées ne sont pas toutes exponentielles, certains cas seulement ont été résolus en mettant en évidence un processus semi-markovien (P S M)

3 3 3 Second type de modèle : composants non identiques

Pour connaître l'état du système il faut alors préciser quels composants sont dans tel ou tel état c est-à-dire connaître en quel point le système se trouve. Le nombre de variables dont dépend la fonction de structure est d'autant plus élevé que le nombre de types de composants est plus grand

L'outil mathématique utilisé est la théorie des P S M à un nombre fini d'états Cette théorie permet de déterminer les transformées de Laplace des distributions des durées des états du système

L'idée générale de la théorie est de conserver le caractère markovien du comportement du système ; plus précisément de choisir les instants de transition d'un état à un autre pour qu'en chacun de ces instants le nouvel état "résume" exhaustivement l'histoire du système

Quand toutes les lois des durées des états des composants sont exponentielles les résultats de la référence [1] s'appliquent parfaitement. Dans le cas contraire, on aboutit seulement s'il existe un choix d'instants de transition qui ne détruise pas le caractère markovien du processus.

4.- MODELE A COMPOSANTS IDENTIQUES

4.1. Hypothèses du modèle

4.1.1. Hypothèses sur les composants

Les durées de fonctionnement des composants sont des variables aléatoires indépendantes de loi exponentielle de paramètre a. Cela signifie que le quantité $a.\Delta t$ est la probabilité conditionnelle qu'un composant tombe en panne dans l'intervalle théoriquement infinitésimal $(t, t + \Delta t)$ sachant qu'il était encore en fonctionnement à l'instant t. Le nombre a, appelé taux de panne, est supposé constant et commun à tous les éléments.

De même les durées d'indisponibilité des composants sont des variables aléatoires indépendantes de loi exponentielle de paramètre b, appelé taux de "réparation".

4.1.2. Hypothèses sur la structure

1°) - le système comprend N composants identiques.

2°) - L'état du système ne dépend que du nombre i de composants indisponibles.

Soient i_1 et i_2 deux valeurs de i telles que : $i_1 < i_2$. Notant E_1, E_r et E_2 les trois états du système respectivement le fonctionnement à charge nominale, le fonctionnement à charge réduite égale à r°/. de la charge nominale et l'indisponibilité totale, la fonction de structure f s'écrit :

$$f(i) = E_1 \quad \text{si} \quad i < i_1$$

$$= E_r \quad \text{si} \quad i_1 \leqslant i < i_2$$

$$= E_2 \quad \text{si} \quad i = i_2$$

car nous allons voir que le cas $i > i_2$ n'est pas possible

3°) - Terminons par les règles de gestion , notons n le nombre maximal de composants fonctionnant simultanément en F Cinq cas sont à envisager selon la valeur de i précédant immédiatement une fin de fonctionnement ou d'indisponibilité.

a) - $i < N - n$ (S non vide, F plein)

Tout composant sortant de R va en S.

Tout composant sortant de F va en R ; il est instantanément remplacé par un composant venant de S

b) - $i = N - n$ (S vide, F plein)

Tout composant sortant de R va en S.

Tout composant sortant de F va en R ; il n'est pas remplacé.

c) - $N - n < i < i_2 - 1$ (S vide, F non plein en fonctionnement)

Tout composant sortant de R va en F.

Tout composant sortant de F va en R ; il n'est pas remplacé.

d) - $i = i_2 - 1$ (S vide, F non plein en fonctionnement limite)

Tout composant sortant de R va en F.

Tout composant sortant de F va en R ; il n'est pas remplacé ; les $N - i_2$ autres composants de F vont en S.

...

e) - $i = i_2$ (E non vide sauf si $i_2 = N$ F totalement indisponible et vide).

Tout composant sortant de E va en F ; les $N - i_2$ composants de S vont également en F

Aucun composant ne peut tomber en panne puisque F est vide ; le cas $i > i_2$ n'est donc pas possible

Remarques :

1°) - F comprend toujours le maximum de composants disponibles sans toutefois dépasser n

2°) - Il peut être logique de poser $i_1 = N - n+1$, si l'on admet que n est calculé tout juste pour que F assure la charge nominale ou bien s'il s'agit d'un système dit "en série" (on devra alors poser de plus $i_2 = i_1$) Mais en règle générale $i_1 \geq N - n+1$

3°) - Pour un système dit "en parallèle" on aura : $i_1 = i_2 = N$

4°) - Plus généralement on pourrait introduire d'autres seuils i_3, i_4 etc correspondant à différents types de fonctionnement à charge réduite

4 2 Application des rappels théoriques au modèle

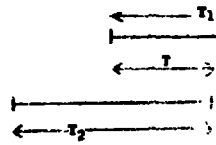
Utilisons la théorie des processus de vie et de mort où l'état du processus est défini par le nombre i de composants indisponibles en ce sens l'état i du processus correspond à un ensemble de $\binom{N}{i}$ points (toutes les configurations des états des composants correspondant à i composants indisponibles)

4 2.1 Détermination des a_i et b_i

Si T_1 est une durée aléatoire de loi exponentielle de paramètre λ_1

Si T_2 " " " λ_2

et si T_1 et T_2 sont indépendantes en probabilité



alors la durée T commune aux deux durées T_1 et T_2 suit quand elle n est pas nulle une loi exponentielle de paramètre $\lambda_1 + \lambda_2$ Ceci résulte simplement

1°) - de l'invariance par troncature à gauche d'une loi exponentielle

2°) - du calcul du minimum de deux variables aléatoires indépendantes

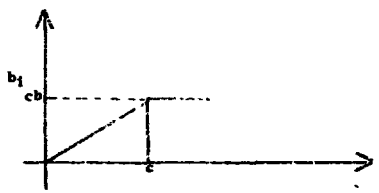
Par suite

$$\begin{cases} a_i = n\,a & \text{si } i \leqslant N-n \\ \quad = (N-i)\,a & \text{si } N-n \leqslant i < i_2 \\ \quad = 0 & \text{si } i = i_2 \\ b_i = i\,b \end{cases}$$

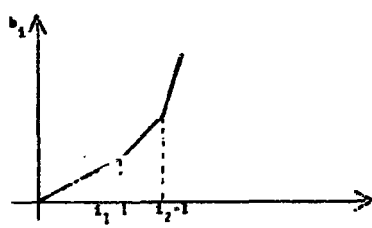
Si ces résultats paraissent discutables, c'est que les hypothèses sur lesquelles ils reposent le sont, à savoir

- lois exponentielles
- indépendance des durées
- "capacité" toujours suffisante du service R.

En particulier si l indépendance des durées d indisponibilité qui entraîne la linéarité du taux b_i paraît irréaliste, il faut estimer les b_i par observation du système au lieu d'estimer b par observation d'un composant ; d ailleurs l'hypothèse classique d'une "capacité" c limitée du service R ($c < i_2$ pour notre modèle) revient au fond à supposer une dépendance très forte entre les durées d'indisponibilité à partir d'un certain seuil



Mais on peut de manière tout aussi réaliste imaginer un taux b_i qui soit modulé en fonction de la situation par exemple



un service R d'autant plus efficace que la situation est plus tendue.

En première analyse, il faudrait voir si on peut distinguer entre les composants qu'on répare et ceux qu'on remplace. Pour ceux qu'on remplace, il serait alors intéressant de voir ceux qu'on peut stocker en magasin (constituant ainsi des composants en réserve non installés pour lesquels durée d'indisponibilité = délai de remplacement et les autres pour lesquels durée d'indisponibilité = délai d'approvisionnement, voire de fabrication).

Dans ces exemples, c'est la manière dont b_i dépend de i que l'on met en cause (c'est-à-dire, en fait l'hypothèse d'indépendance des durées d'indisponibilité) et non l'hypothèse de lois exponentielles (suivant laquelle b_i ne dépend pas du temps).

4.2.2 Probabilités et disponibilité du système en régime limite (cf. référence [4]).

Exprimons les probabilités $P_j^* = \lim_{t\to\infty} P_{ij}(t)$ compte tenu des valeurs de a_i et b_i :

1°) $j \in [0, N-n]$: $P_j^* = C_1 \left(\frac{n\,a}{b}\right)^j \frac{1}{j!}$

(troncature d'une loi de Poisson de paramètre $\frac{n\,a}{b}$).

2°) $j \in [N-n, i_2-1]$: $P_j^* = C_2 \binom{N}{j} \frac{a^j\, b^{N-j}}{(a+b)^N}$

(troncature d'une loi binomiale de paramètre $\frac{a}{a+b}$ définie sur $[0,N]$).

3°) $j = i_2$: $P_j^* = P_{i2}^*$

Les constantes C_1 et C_2 sont choisies pour que les expressions précédentes soient égales en N-n et pour que :

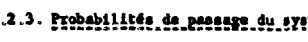
$$\sum_{j=0}^{i_2} P_j^* = 1$$

...

En régime limite la disponibilité du système vaut alors :

$$D = P^{\infty}[E_1] + \frac{r}{100}\, P^{\infty}[E_r] = \sum_{j=0}^{i_1-1} P^{\infty}_j + \frac{r}{100} \sum_{j=i_1}^{i_2-1} P^{\infty}_j$$

4.2.3. Probabilités de passage du système (en régime limite)



Le système pouvant prendre trois états E_1, E_r et E_2, on va déterminer une de ses caractéristiques de fiabilité : la matrice des probabilités de passage d'un état à l'autre. Quittant l'état E_1, le système a la probabilité 1 de prendre l'état E_r ; de même quittant E_2 il entre nécessairement en E_r. Mais quittant E_r, le système peut aller soit en E_1, soit en E_2 avec des probabilités P_1 et P_2 que nous allons déterminer en nous plaçant en régime limite.

La nécessité de se placer en régime limite vient de ce que la connaissance de l'état de départ, ici E_r, n'est pas suffisante pour déterminer P_1 ou P_2 dans le cas général ; en effet quand le système quitte l'état E_r entre l'instant t et l'instant t+dt, le processus se trouve en t, soit dans l'état $i = i_1$, soit dans l'état $i = i_2-1$.

Or en général la probabilité pour que le processus se trouve dans un état donné dépend des états antérieurs ($P_{ij}(t)$ dépend en général de i) si bien que la détermination de P_1 et de P_2 exige une information plus fine que la seule connaissance de E_r ; mais puisque nous désirons étudier les états du système il faut constater que le processus n'est en général plus markovien à ce niveau d'identification.

En revanche, si l'on se place en régime limite, on sait déterminer dans le cas positivement régulier la probabilité de se trouver dans un état donné du processus : $P^{\infty}_j = \lim_{t\to\infty} P_{ij}(t)$ qui ne dépend plus de i.

...

Alors l'évènement conditionnant A_r "le système quitte E_r entre t et t+dt" a pour probabilité :

$$P^*_{i_1} \cdot b_{i_1} \cdot dt + P^*_{i_2-1} \cdot a_{i_2-1} \cdot dt$$

La probabilité de l'évènement A_1 "le système va en E_1 entre t et t+dt" vaut $P^*_{i_1} \cdot b_{i_1} \cdot dt$

La probabilité de l évènement A_2 "le système va en E_2 entre t et t+dt" vaut $P^*_{i_2-1} \cdot a_{i_2-1} \cdot dt$

Les probabilités cherchées sont les probabilités conditionnelles

$$P(A_1 / A_r) \quad \text{et} \quad P(A_2 / A_r)$$

$$P_1 = \frac{P^*_{i_1} \cdot b_{i_1}}{P^*_{i_1} \cdot b_{i_1} + P^*_{i_2-1} \cdot a_{i_2-1}} = \frac{1}{1 + (\frac{a}{b})^{i_2-i_1} \frac{\binom{N}{i_2}}{\binom{N}{i_1}}}$$

$$P_2 = \frac{1}{1 + (\frac{b}{a})^{i_2-i_1} \frac{\binom{N}{i_1}}{\binom{N}{i_2}}}$$

Dans le cas particulier où $i_2-1 = i_1$, on retrouve les valeurs classiques :

$$\frac{b_{i_1}}{b_{i_1} + a_{i_1}} \quad \text{et} \quad \frac{a_{i_1}}{b_{i_1} + a_{i_1}}$$

qui sont exactes même en régime non limite puisque l'état E_r du système se réduit à un seul état du processus de vie et de mort.

En résumé la matrice des probabilités de passage s'écrit :

	E_1	E_r	E_2
E_1	0	1	0
E_r	P_1	0	P_2
E_2	0	1	0

4.2.4. Lois des durées des états du système (en régime limite)

Si l'état initial du système est E_r ou E_2, la fonction de répartition de la durée de l'état E_1 est donnée, avec les notations précédentes, par $G_{i_1\ 1,\ i_1}(t)$

Si en revanche, l'état initial du système est E_1, il faut préciser l'état initial i_o du processus : la première durée de l'état E_1 a pour fonction de répartition $G_{i_o i_1}(t)$ et les durées suivantes $G_{i_1-1, i_1}(t)$.

La fonction de répartition de la durée de l'état E_2 vaut $G_{i_2,\ i_2-1}(t)$ et l'on retrouve la loi exponentielle de paramètre $i_2 b$

Le cas de l'état E_r est plus complexe : les fonctions G_{i_1,i_1-1} et $G_{i_2-1,\ i_2}$ sont en effet relatives aux durées des états $(E_r \bigcup E_2)$ et $(E_r \bigcup E_1)$. Il est nécessaire de décomposer la durée de l'état E_r selon qu'elle est précédée et suivie de durées des états E_1 ou E_2 ; cette remarque revient à constater que le processus au niveau des états du système n'est plus markovien ou plutôt qu'il est markovien d'ordre deux :

Etat précédent :		E_1	E_2	Cadre du Calcul
Etat suivant	E_1	$\bar{G}_{i_1,i_1-1}$	$\bar{G}_{i_2-1,\ i_1-1}$	$i \neq i_2$
	E_2	$G_{i_1,\ i_2}$	$G_{i_2-1,\ i_2}$	$i \geqslant i_1$

(Les fonctions intervenant dans la loi de durées de E_r sont celles du tableau. On les a surlignées ou soulignées pour signifier que leur détermination doit être effectuée en prenant soin de renuméroter les états du processus de manière à rendre les états E_2 ou E_1 inaccessibles).

Plaçons-nous en régime limite pour pouvoir lever le conditionnement sur l'état précédent et retrouver un système markovien.

En régime limite (relation $P^*_{j+1} \cdot b_{j+1} = P^*_j \cdot a_j$) la probabilité de venir de E_1 sachant qu'on entre en E_r est égale à la probabilité d'aller en E_1 sachant qu'on vient de E_r ; de même pour E_2.

Par conséquent, la fonction de répartition de la durée de l'état E_r suivie de l'état E_1 s'écrit :

$$P_1 \bar{G}_{i_1,i_1-1}(t) + P_2 \bar{G}_{i_2-1,\ i_1-1}(t)$$

...

De même la fonction de répartition de la durée de l'état E_r suivie de l'état E_2 vaut

$$P_1 \, G_{i_1, i_2}(t) \quad + \quad P_2 \, G_{i_2-1, i_2}(t)$$

On dispose ainsi des deux matrices (celle des probabilités de passage et celle des fonctions de répartition des durées) caractérisant un processus semi-markovien à 3 états.

Ce type de calcul s'étend sans difficulté à un nombre quelconque d'états tels que E_r compris entre E_1 et E_2, les seuls passages vers les 2 états adjacents étant possibles.

4.2.5. Durées moyennes des états du système

La détermination des durées moyennes de E_1 peut s'effectuer grâce aux formules indiquées dans les rappels théoriques.

On propose ici une méthode directe qui permet de plus de déterminer la durée moyenne de l'état E_r et s'inspire de la référence [4].

La durée moyenne de l'état E_i peut s'écrire:

$$\frac{\text{Durée moyenne par unité de temps de l'état } E_i}{\text{Nombre moyen par unité de temps de passages par l'état } E_i}$$

Le numérateur est égal à la probabilité limite $P^*(E_i)$ de l'état E_i.

Le dénominateur est égal à la probabilité limite divisée par dt pour que le système prenne l'état E_i entre t et t + dt.

...

La durée moyenne de l'état E_r vaut donc :

$$\frac{\sum_{j=i_1}^{i_2-1} P_j^*}{P_{i_1-1}^* \; a_{i_1-1} + P_{i_2}^* \; b_{i_2}} = \frac{\sum_{j=i_1}^{i_2-1} \rho_j}{\rho_{i_1} \; b_{i_1} + \rho_{i_2-1} \; a_{i_2-1}}$$

4 3. **Exemples**

Traitons 2 exemples très simples mettant en évidence la facilité d'obtention des polynômes $Q_K(x)$

4 3 1. Cas $N = n = 2$, $i_1 = i_2 = 2$

$$a_0 = 2a \qquad b_0 = 0$$

$$a_1 = a \qquad b_1 = b$$

$$a_2 = 0 \qquad b_2 = 2b$$

$$P_j^* = \binom{N}{j} \left(\frac{a}{a+b}\right)^j \left(\frac{b}{a+b}\right)^{N-j}$$

La disponibilité du système vaut en régime limite

$$D = P_0^* + P_1^* = \left(\frac{b}{a+b}\right)^2 + 2\,\frac{ab}{(a+b)^2} = \frac{b(b+2a)}{(a+b)^2}$$

Or : $d = \frac{\frac{1}{a}}{\frac{1}{a} + \frac{1}{b}}$ est la disponibilité en régime limite d'un composant puisque $\frac{1}{a}$ représente sa durée moyenne de fonctionnement, $\frac{1}{b}$ sa durée moyenne d'indisponibilité et que l'état de réserve n'existe pas (cas N = n)

$$1 - D = (1 - d)^2$$

C'est en ce sens que pour calculer la disponibilité du système, la seule caractéristique d de fiabilité des composants suffit dans ce cas ; mais il est clair que, dès qu'il y a réserve (N > n) la disponibilité d des composants est une donnée insuffisante pour calculer la disponibilité du système (voir l'exemple 3 2).

Les relations de récurrence données dans les rappels théoriques permettent d'écrire :

$$Q_0(x) = 1$$

$$Q_1(x) = \frac{2a - x}{2a}$$

$$Q_2(x) = \frac{1}{2a^2} x^2 - \frac{1}{2a^2} (3a + b) x + 1$$

Vérifions d'abord que la durée de l'état E_2 (indisponibilité) du système suit une loi exponentielle de paramètre 2b ; la transformée de Laplace de la densité de cette loi vaut :

$$g_{21}(s) = \frac{\bar{Q}_{2-2}(-s)}{\bar{Q}_{2-1}(-s)} = \frac{1}{\frac{2b + s}{2b}} = \frac{2b}{2b + s}$$

La densité vaut donc $z_{21}(t) = 2b \cdot e^{-2bt}$ et la durée moyenne de l'état E_2 : 1/2 b.

...

De même la transformée de Laplace de la densité de la durée de l'état E_1 (fonctionnement) du système vaut :

$$S_{12}^*(s) = \frac{Q_1(-s)}{Q_2(-s)} = \frac{\frac{2a+s}{2a}}{\frac{1}{2a^2}s^2 + \frac{1}{2a^2}(3a+b)s + 1}$$

$$S_{12}^*(s) = \frac{s(2a+s)}{(s+s_1)(s+s_2)}$$

où s_1 et s_2 sont les zéros de $Q_2(s)$

$$S_{12}^*(s) = \frac{s}{s_2 - s_1}\left[\frac{2a - s_1}{s + s_1} - \frac{2a - s_2}{s + s_2}\right]$$

$$\text{et } S_{12}(t) = \frac{s}{s_2 - s_1}\left[(2a - s_1)\, e^{-s_1 t} - (2a - s_2)\, e^{-s_2 t}\right]$$

La durée moyenne de l'état E_1 vaut :

$$\int_0^\infty t.S_{12}(t)\,dt = \frac{s}{s_2 - s_1}\left(\frac{2a - s_1}{s_1^2} - \frac{2a - s_2}{s_2^2}\right) = \frac{2a + b}{2a^2}$$

...

4 3.2. Cas N = 2, n = 1, $i_1 = i_2 = 2$

$$a_0 = a \qquad b_0 = 0$$

$$a_1 = a \qquad b_1 = b$$

$$a_2 = 0 \qquad b_2 = 2b$$

$$P_0^* = \frac{2b^2}{2b^2 + 2ab + a^2}$$

$$D = P_0^* + P_1^* = \frac{2b^2 + 2ab}{2b^2 + 2ab + a^2}$$

$$P_1^* = \frac{2ab}{2b^2 + 2ab + a^2}$$

$$1 - D = \frac{a^2}{2b^2 + 2ab + a^2}$$

$$P_2^* = \frac{a^2}{2b^2 + 2ab + a^2}$$

La valeur de 1 - D trouvée est plus petite que dans l'exemple précédent $\left(\frac{a^2}{b^2 + 2ab + a^2}\right)^2$; la disponibilité du système de l'exemple 4 3 2. est plus grande que celle du système 4 3.1 Il n'est donc pas indifférent quand on dispose de deux composants identiques dont un seul assure le pleine charge du système (dans les deux cas) de les faire fonctionner simultanément "en parallèle" ou d'en garder un systématiquement en réserve quand les deux sont disponibles. Si, comme on l'a supposé dans ce modèle, le passage de la réserve au fonctionnement (la commutation) se fait sans aucun risque d'indisponibilité, le système "avec réserve" a une meilleure disponibilité

Déterminons les polynômes :

$$Q_0(x) = 1$$

$$Q_1(x) = \frac{a - x}{a}$$

$$Q_2(x) = \frac{1}{a^2} x^2 - \frac{1}{a^2} (2a + b) x + 1$$

La durée de l'état E_2 suit, dans cet exemple aussi, une loi exponentielle de paramètre 2b.

La transformée de Laplace de la densité de la durée de E_1 s'écrit :

$$g^*_{12}(s) = \frac{\frac{s + a}{a}}{\frac{s^2 + (2a + b)\, s + a^2}{a^2}}$$

$$= \frac{a}{s_2 - s_1} \left[\frac{s - s_1}{s + s_1} - \frac{s - s_2}{s + s_2} \right]$$

où s_1 et s_2 sont les zéros de $Q_2(s)$

$$g_{12}(t) = \frac{a}{s_2 - s_1} \left[(a - s_1)\, e^{-s_1 t} - (a - s_2)\, e^{-s_2 t} \right]$$

La durée moyenne de E_1 vaut $\frac{a + b}{a^2} = \frac{1}{a} + \frac{b}{a^2}$ qui est supérieure à la durée correspondante de l'exemple précédent qui valait $\frac{1}{a} + \frac{b}{2a^2}$.

...

4.4. Cas de lois non-exponentielles

Le cas général (N et n quelconques, lois quelconques des durées d'état des composants) ne saurait être résolu à l'aide de la théorie des processus semi-markoviens puisqu'en général il n'existe pas un choix d'instants de changement d'état qui conserve le caractère markovien du processus ; en effet, l'état du système dépend en général des dates d'entrée dans le service F ou dans le service R : dates du début du fonctionnement et du début de "réparation" des différents composants.

Il existe cependant quelques cas particuliers qui ont été résolus après avoir mis en évidence l'existence d'un processus semi-markovien ; nous en citerons deux.

4.4.1. Cas N = n = 1, $i_1 = i_2 = 1$, lois quelconques des durées de fonctionnement et d'indisponibilité.

Le système est constitué d'un seul composant qui est mis en "réparation" dès qu'il tombe en panne et en fonctionnement dès qu'il redevient disponible. On a affaire à un processus dit de renouvellement alterné (référence [5], chapitre 7) où les 2 états (fonctionnement et indisponibilité) se succèdent de manière systématique sans qu'on ait alors besoin de déterminer la matrice de passage. On peut dire de manière équivalente qu'il s'agit d'un processus semi-markovien à 2 états.

On peut alors utiliser les résultats de l'une ou l'autre théorie (renouvellement, semi-markovien) pour obtenir les caractéristiques de fiabilité du système. Ce cas est traité à la référence [2], chapitre 3, section 6.

...

4.4.2. Cas N quelconque, $n = i_t \ldots i_1 \ldots i_2 = N$, loi quelconque des durées de fonctionnement, loi exponentielle des durées d'indisponibilité.

Des cas ayant même structure stochastique ont été résolus aux références [6] et [7]

On indiquera seulement quels sont les instants de passage de la "chaîne" de Markov associée au processus ; ces instants sont ceux précédent immédiatement (ou suivant immédiatement) une panne (c'est-à-dire une fin de fonctionnement) de l'unique composant qui peut être en fonctionnement ; en effet, X(t) représentant le nombre de composants indisponibles, si t_n et t_{n+1} sont deux instants consécutifs du type précédent, la probabilité

$$P\left[X(t_{n+1}) = j \,/\, X(t_n) = i \right]$$

ne dépend que de i, j et de la différence $(t_{n+1} - t_n)$.

En effet :

$j = i$ - nombre de composants "réparés" entre t_n et $t_{n+1}+1$; or la probabilité d'un nombre K donné de composants "réparés" pendant le temps $(t_{n+1} - t_n)$ est donnée par la fonction de répartition de la variable aléatoire U_k^i : kième par ordre croissant de i réalisations indépendantes d'une variable aléatoire de loi exponentielle avec la relation $K = i-j+1$.

5.- MODELES A COMPOSANTS NON-IDENTIQUES

5.1. Hypothèses des modèles

Dans les deux modèles traités, on ne considérera que deux composants (1) et (2), dont les durées de fonctionnement suivront des lois exponentielles de paramètres respectifs a_1 et a_2 et les durées d'indisponibilité des lois exponentielles de paramètres respectifs b_1 et b_2. Toutefois, dans le premier modèle, on pourra considérer une probabilité non nulle de tomber en panne au début du fonctionnement. Les fonctions de structure et les règles de gestion seront précisées pour chacun des modèles.

Nous allons utiliser la théorie des processus semi-markoviens, alors que dans le cas de composants identiques l'état du processus était caractérisé par le nombre de composants indisponibles et correspondait à un ensemble de points, l'état du processus sera ici caractérisé par la configuration des états des composants, c'est-à-dire par un point ; c'est ce mot "point" que l'on emploiera dans les modèles pour éviter toute confusion.

L'essentiel des résultats, obtenus sous une forme et par une méthode différentes, figure à la référence [8] .

5.2. Premier modèle

5.2.1. Fonction de structure et règles de gestion

Les états du système sont au nombre de 2 :

E_1 : fonctionnement à charge nominale

E_2 : indisponibilité totale

Les points sont au nombre de 3

α : (1) et (2) fonctionnent

β : (1) est en réserve, (2) est indisponible

γ : (1) est indisponible, (2) est en réserve.

La non-identité des 2 composants exige un point de plus.

La fonction de structure f s'écrit :

$f(\alpha) = E_1$

$f(\beta) = f(\gamma) = E_2$

Règles de gestion

a) - Point α.

Tout composant sortant de F va en R.

L'autre composant va en S.

b) - Points β ou γ.

Le composant sortant de R va en F.

L'autre, soit (i) va de S en F mais a la probabilité ε_i d'y rester un temps nul pour aller en R (donc pratiquement d'aller directement en R). Le composant sortant de R a donc la probabilité ε_i d'aller en F, d'y rester un temps nul pour aller en S. Le composant (i) à la probabilité $1 - \varepsilon_i$ de séjourner en F pendant une durée non nulle.

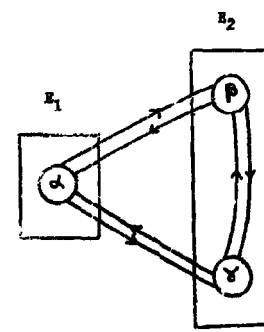
Autrement dit, si $\varepsilon_i \neq 0$, la commutation réserve $\longrightarrow$ fonctionnement du composant (i) n'est pas parfaitement fiable.

On peut résumer ces hypothèses en disant qu'on a affaire à un système "en série" ; à ce niveau la généralisation du modèle à N composants non-identiques ne pose pas de problème.

5.2.2. La matrice $Q^*(s)$

Traduisons les hypothèses précédentes à l'aide de la théorie des P.S.M. où les états du processus sont les points α, β, γ :

	α	β	γ
α	0	$\frac{a_2}{a_1 + a_2}$	$\frac{a_1}{a_1 + a_2}$
$\beta = \beta$	$1 - \varepsilon_1$	0	ε_1
γ	$1 - \varepsilon_2$	ε_2	0



$\gamma(t)$ \ α	α	β	γ
α	arbitraire	$1-e^{-(a_1+a_2)t}$	$1-e^{-(a_1+a_2)t}$
β	$1-e^{-b_2 t}$	arbitraire	$1-e^{-b_2 t}$
γ	$1-e^{-b_1 t}$	$1-e^{-b_1 t}$	arbitraire

Ecrivons directement la matrice des transformées de LAPLACE des densités de transition, en omettant désormais d'expliciter les états du processus :

$$q^*(s) = \begin{bmatrix} 0 & \dfrac{a_2}{s+a_1+a_2} & \dfrac{a_1}{s+a_1+a_2} \\ \dfrac{(1-\psi_1)\,b_2}{s+b_2} & 0 & \dfrac{\psi_1\, b_2}{s+b_2} \\ \dfrac{(1-\psi_2)\,b_1}{s+b_1} & \dfrac{\psi_2\, b_1}{s+b_1} & 0 \end{bmatrix}$$

5.2.3. Lois des durées des états du système

La loi de la durée de l'état E_1 est, sans calcul, une loi exponentielle de paramètre $(a_1 + a_2)$.

La transformée de LAPLACE de la densité de la durée de l'état E_2 s'écrit :

$$F_{\alpha\beta}\; s^*_{\beta\alpha}(s) + F_{\alpha\gamma}\; s^*_{\gamma\alpha}(s)$$

...

En effet seule la loi marginale de la durée de l'état E_2 importe puisqu'on ne désire pas distinguer les points β et γ au sein de l état E_2 du système ; par ailleurs la transformation de LAPLACE est linéaire.

On obtient simplement $g^*_{\alpha\beta}(s)$ et $g^*_{\alpha\gamma}(s)$ en écrivant la matrice $\left[I - q^*(s)\right]^{-1}$ sous la forme :

$$\left[I - q^*(s)\right]^{-1} = \frac{1}{\Delta} \begin{bmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{bmatrix}$$

Soit, après calcul :

$$g^*_{\alpha\beta}(s) = \frac{(1 - \gamma_1)\, b_2}{s + b_2} + \frac{\gamma_1\, b_2}{s + b_2} \cdot \frac{x_3}{x_1}$$

et $$g^*_{\alpha\gamma}(s) = \frac{(1 - \gamma_2)\, b_1}{s + b_1} + \frac{\gamma_2\, b_1}{s + b_1} \cdot \frac{x_2}{x_1}$$

où x_1, x_2 et x_3 sont les cofacteurs des éléments de la première ligne de $1 - q^*(s)$.

Soit pour la transformée de LAPLACE de la densité de la durée de E_2 .

$$\frac{1}{a_1 + a_2} \left[\frac{s\left[a_1 b_1 (1 - \gamma_2) + a_2 b_2 (1 - \gamma_1)\right] + b_1 b_2 (a_1 + a_2)(1 - \gamma_1 \gamma_2)}{s^2 + s(b_1 + b_2) + b_1 b_2 (1 - \gamma_1 \gamma_2)} \right.$$

Les racines s_1 et s_2 du dénominateur sont réelles, négatives et $-b_1$, $-b_2$ appartiennent à l'intervalle (s_1, s_2). La densité est une combinaison linéaire de deux exponentielles décroissantes

Dans le cas particulier où $\mathcal{C}_1 = \mathcal{C}_2 = 0$, la transformée de LAPLACE devient :

$$\frac{a_1}{a_1 + a_2} \cdot \frac{b_1}{s + b_1} + \frac{a_2}{a_1 + a_2} \cdot \frac{b_2}{s + b_2}$$

et la densité de la durée de l'état E_2 :

$$\frac{a_1}{a_1 + a_2} b_1 e^{-b_1 t} + \frac{a_2}{a_1 + a_2} b_2 e^{-b_2 t}$$

5.2.4. Valeurs moyennes et disponibilité du système

Plutôt que d'obtenir les durées moyennes à partir des transformées de LAPLACE des lois par les moyens classiques, on peut les calculer directement en utilisant la chaîne de Markov associée dont on détermine les probabilités en régime limite :

$$\pi_\alpha = \frac{(a_1 + a_2)(1 - \mathcal{C}_1 \mathcal{C}_2)}{a_1 \mathcal{C}_2 + a_2 \mathcal{C}_1 + (2 - \mathcal{C}_1 \mathcal{C}_2)(a_1 + a_2)}$$

$$\pi_\beta = \frac{a_2 + a_1 \mathcal{C}_2}{a_1 \mathcal{C}_2 + a_2 \mathcal{C}_1 + (2 - \mathcal{C}_1 \mathcal{C}_2)(a_1 + a_2)}$$

$$\pi_\gamma = \frac{a_1 + a_2 \mathcal{C}_1}{a_1 \mathcal{C}_2 + a_2 \mathcal{C}_1 + (2 - \mathcal{C}_1 \mathcal{C}_2)(a_1 + a_2)}$$

...

Notant $\theta_\alpha = \frac{1}{a_1 + a_2}$, $\theta_\beta = \frac{1}{b_2}$ et $\theta_\gamma = \frac{1}{b_1}$ les durées moyennes des points α, β et γ sans qu'il y ait de confusion possible avec θ_1 et θ_2, on sait que :

$$\ell_{\alpha\alpha} = \frac{1}{\pi_\alpha} \sum_{\kappa = \alpha, \beta, \gamma} \pi_\kappa \cdot \theta_\kappa$$

$$\ell_{\alpha\alpha} = \frac{(1 - \theta_1 \theta_2) b_1 b_2 + a_2 + a_1 \theta_2) b_1 + (a_1 + a_2 \theta_1) b_2}{(a_1 + a_2)(1 - \theta_1 \theta_2) b_1 b_2}$$

$$\ell_{\beta\beta} = \frac{(1 - \theta_1 \theta_2) b_1 b_2 + (a_2 + a_1 \theta_2) b_1 + (a_1 + a_2 \theta_1) b_2}{(a_2 + a_1 \theta_2) b_1 b_2}$$

$$\ell_{\gamma\gamma} = \frac{(1 - \theta_1 \theta_2) b_1 b_2 + (a_2 + a_1 \theta_2) b_1 + (a_1 + a_2 \theta_1) b_2}{(a_1 + a_2 \theta_1) b_1 b_2}$$

Ces durées moyennes ont un intérêt pratique important en régime limite .

$\frac{1}{\ell_{\alpha\alpha}}$ représente l'espérance du nombre de démarrages effectifs par unité de temps.

$\frac{1}{\ell_{\beta\beta}}$, par exemple, représente l'espérance du nombre de réparations (ou de remplacements) effectuées sur le composant (2) par unité de temps.

...

La durée moyenne de l'état E_2 se déduit de $\ell_{\alpha,\alpha}$ en retranchant $\psi_{\alpha\alpha}$:

$$\ell_{\alpha,\alpha} - \psi_{\alpha\alpha} = \frac{a_2 b_1 + a_1 b_1 \quad \psi_2 + a_1 b_2 + a_2 b_2 \quad \psi_1}{(a_1 + a_2)(1 - \psi_1 \psi_2) b_1 b_2}$$

On a vu qu'on peut également obtenir cette durée moyenne en rendant le point α absorbant et en considérant la matrice :

$$I - \bar{P} = \begin{bmatrix} 1 & - \psi_1 \\ - \psi_2 & 1 \end{bmatrix}$$

et son inverse :

$$(m_{ij}) = \frac{1}{1 - \psi_1 \psi_2} \begin{bmatrix} 1 & \psi_1 \\ \psi_2 & 1 \end{bmatrix}$$

La durée moyenne de E_2 est alors la moyenne pondérée des durées correspondant aux entrées soit dans l'état β, soit dans l'état γ :

$$P_{\alpha\beta} \cdot \sum_{k=\beta,\gamma} m_{\beta k} \cdot \psi_k + P_{\alpha\gamma} \sum_{k=\beta,\gamma} m_{\gamma k} \psi_k$$

expression qui redonne le résultat précédent.

On peut enfin exprimer la disponibilité D du système en régime limite à l'aide des durées moyennes des états E_1 et E_2 :

$$D = \frac{\frac{1}{a_1 + a_2}}{\frac{1}{a_1 + a_2} + \frac{a_2 b_1 + a_1 b_1 \psi_2 + a_1 b_2 + a_2 b_2 \psi_1}{(a_1 + a_2)(1 - \psi_1 \psi_2) b_1 b_2}}$$

$$D = \frac{b_1 b_2 (1 - \psi_1 \psi_2)}{b_1 b_2 (1 - \psi_1 \psi_2) + a_1 b_2 + a_2 \psi_2 b_1 + a_2 (b_1 + \psi_1 b_2)}$$

De manière équivalente D est égale à la probabilité limite $P^*_{\alpha\alpha}$ pour que le processus semi-markovien soit dans l'état α :

$$P^*_{\alpha\alpha} = \frac{\psi_{\alpha\alpha}}{\ell_{\alpha\alpha}}$$

Dans le cas particulier où $\psi_1 = \psi_2 = 0$, notons la relation simple, évidente à généraliser :

$$\frac{\text{Durée moyenne d'indisponibilité du système}}{\text{Durée moyenne de fonctionnement du système}} = \sum_{i=1,2} \frac{\text{durée moyenne d'indisponibilité du composant } i}{\text{durée moyenne de fonctionnement du composant } i}$$

5.3. Second modèle

5.3.1. Fonction de structure et règles de gestion

Il y a 2 états du système :

- E_1 : fonctionnement à charge nominale
- E_2 : indisponibilité totale

Il y a 4 points :

α : (1) et (2) fonctionnent

β : (1) fonctionne, (2) est indisponible

γ : (1) est indisponible, (2) fonctionne

δ : (1) et (2) sont indisponibles.

La non-identité des 2 composants exige un point de plus.

La fonction de structure s'écrit :

$f(\alpha) = f(\beta) = f(\gamma) = E_1$

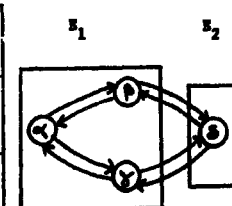
$f(\delta) = E_2$

Les règles de gestion sont simples : il n'y a pas de réserve ($\mathcal{E}$ est toujours vide) ; quel que soit le point où l'on se trouve, tout composant sortant de $\mathcal{F}$ va en $\mathcal{R}$ et tout composant sortant de $\mathcal{R}$ va en $\mathcal{F}$; ces sauts n'ont aucune incidence sur ceux de l'autre composant : les gestions des 2 composants sont indépendantes. En bref, il s'agit d'un système "en parallèle".

5.3.2. La matrice $q^{\mathcal{B}}(s)$

Comme pour le modèle précédent, le P.S.M. a pour états les points α, β, γ et δ :

	α	β	γ	δ
α	0	$\frac{a_2}{a_1 + a_2}$	$\frac{a_1}{a_1 + a_2}$	0
β	$\frac{b_2}{a_1 + b_2}$	0	0	$\frac{a_1}{a_1 + b_2}$
γ	$\frac{b_1}{a_2 + b_1}$	0	0	$\frac{a_2}{a_2 + b_1}$
δ	0	$\frac{b_1}{b_1 + b_2}$	$\frac{b_2}{b_1 + b_2}$	0



...

$F(t) =$

	α	β	γ	δ
α	A	$1-e^{-(a_1+a_2)t}$	$1-e^{-(a_1+a_2)t}$	A
β	$1-e^{-(b_2+a_1)t}$	A	A	$1-e^{-(b_2+a_1)t}$
γ	$1-e^{-(b_1+a_2)t}$	A	A	$1-e^{-(b_1+a_2)t}$
δ	A	$1-e^{-(b_1+b_2)t}$	$1-e^{-(b_1+b_2)t}$	A

A : fonction de répartition arbitraire.

Durées moyennes des états

$$t_\alpha = \frac{1}{a_1 + a_2}$$

$$t_\beta = \frac{1}{b_2 + a_1}$$

$$t_\gamma = \frac{1}{b_1 + a_2}$$

$$t_\delta = \frac{1}{b_1 + b_2}$$

$q^*(s) =$

0	$\frac{a_2}{s + a_1 + a_2}$	$\frac{a_1}{s + a_1 + a_2}$	0
$\frac{b_2}{s + b_2 + a_1}$	0	0	$\frac{a_1}{s + b_2 + a_1}$
$\frac{b_1}{s + b_1 + a_2}$	0	0	$\frac{a_2}{s + b_1 + a_2}$
0	$\frac{b_1}{s + b_1 + b_2}$	$\frac{b_2}{s + b_1 + b_2}$	0

...

5.3.3. Loi des durées des états du système

La loi de la durée de E_2 est évidemment une loi exponentielle de paramètre $(b_1 + b_2)$.

La transformée de LAPLACE de la densité de la durée de E_1 s'écrit :

$$P_{\beta\beta}\ \pi^*_{\beta\delta}\ (s) + P_{\beta\gamma}\ \pi^*_{\gamma\delta}\ (s)$$

Soit, après simplification, pour la transformée de la densité de la durée de E_1 :

$$\frac{1}{+b_2)}\left[\frac{s^2(a_1b_1+a_2b_2)+s\left[a_1b_1(a_1+b_1+2a_2)+a_2b_2(a_2+b_2+2a_1)\right]+(b_1+b_2)a_1a_2\ (a_1+a_2+b_1+b_2)}{s^3+s^2(2a_1+2a_2+b_1+b_2)+s\left[(a_1+a_2)(a_1+a_2+b_1+b_2)+a_1a_2+b_1b_2\right]+a_1a_2(a_1+a_2+b_1+b_2)}\right]$$

Dans le cas particulier où : $a_1 = a_2 = a$

$$b_1 = b_2 = b$$

c'est-à-dire le cas de 2 composants identiques, la quantité $-(s+b)$ est zéro à la fois du numérateur et du dénominateur dont les degrés diminuent chacun d'une unité ; on retrouve la transformée de la densité de la durée de E_1 obtenue à l'exemple 4.3.1.

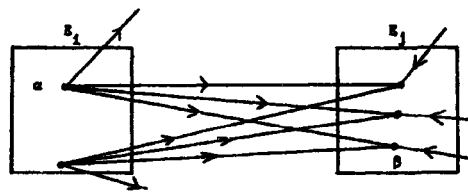
5.3.4. Valeurs moyennes et disponibilité du système

Comme pour le modèle précédent, on calcule les probabilités en régime limite de la chaîne de MARKOV associée :

$$\pi_\alpha = \frac{1}{2}\ \frac{\frac{1}{a_1}+\frac{1}{a_2}}{\frac{1}{a_1}+\frac{1}{a_2}+\frac{1}{b_1}+\frac{1}{b_2}} \qquad \pi_\beta = \frac{1}{2}\ \frac{\frac{1}{b_1}+\frac{1}{b_2}}{\frac{1}{a_1}+\frac{1}{a_2}+\frac{1}{b_1}+\frac{1}{b_2}}$$

...

On se propose donc de déterminer en régime limite la matrice des répartitions de transition des états E_i du système.



La quantité $P^*_\alpha . \lambda_\alpha . P_{\alpha\beta} . dt$ représente la probabilité a priori pour qu'en régime limite le système passe du point α au point β pendant le temps dt

Si l'on pose $$\tau_{ij} = \sum_{\alpha=f^{-1}(E_i)} \sum_{\beta=f^{-1}(E_j)} P^*_\alpha . \lambda_\alpha . P_{\alpha\beta}$$

La probabilité de passage de E_i en E_j vaut :

$$P_{E_i E_j} = \frac{\tau_{ij}}{\sum_{j \neq i} \tau_{ij}}$$

Comme en 4.2.3., le calcul de $P_{E_i E_j}$ ne peut être effectué qu'en régime limite car il nécessite l'identification des points α ayant E_i pour image dans l'application f ; la probabilité pour que le système se trouve en l'un de ces points dépend en régime quelconque des points précédents.

...

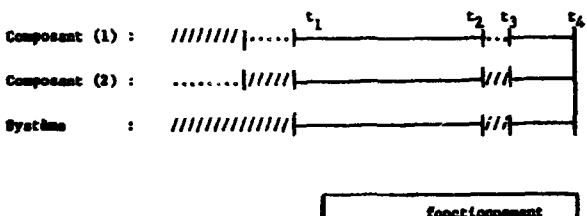
Le calcul de $P_{E_i E_j}$ n'est exact en régime quelconque que si E_i n'est l'image que d'un seul point.

La loi $F_{E_i E_j}(t)$ des durées de l'état E_i suivi de E_j peut s'obtenir à partir des lois $g_{\alpha E_j}$ où les α sont les points ayant E_i pour image dans l'application f ; les lois $g_{\alpha E_j}$ sont déterminées dans le cadre d'un processus ayant pour états : les points α et l'état E_j ; ce processus est obtenu à partir du processus initial en rendant les autres points inaccessibles.

Pour obtenir $F_{E_i E_j}(t)$, il suffit de pondérer les $g_{\alpha E_j}$ par les probabilités en régime limite d'aller en α venant des états du système autres que E_i.

5.5. Cas de lois non-exponentielles

Représentons, dans le cas du premier modèle, les diagrammes fonctionnement-arrêt des 2 composants et du système :



...

$$\pi_\beta = \frac{1}{2} \quad \frac{\frac{1}{a_1} + \frac{1}{b_2}}{\frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{b_1} + \frac{1}{b_2}} \qquad \pi_\gamma = \frac{1}{2} \quad \frac{\frac{1}{a_2} + \frac{1}{b_1}}{\frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{b_1} + \frac{1}{b_2}}$$

Soit :

$$\ell_{\delta\delta} = \frac{1}{\pi_\delta} \qquad \delta = \alpha, \beta, \gamma, \delta \qquad \pi_K \cdot \ell_K$$

$$\ell_{\delta\delta} = \frac{(a_1 + b_1)(a_2 + b_2)}{(b_1 + b_2)\, a_1\, a_2}$$

et la durée moyenne de E_1 vaut :

$$\ell_{\delta\delta} - \ell_\delta = \frac{a_2\, b_1 + a_1\, b_2 + b_1\, b_2}{(b_1 + b_2)\, a_1\, a_2}$$

$$D = \frac{a_2\, b_1 + a_1\, b_2 + b_1\, b_2}{(a_1 + b_1)(a_2 + b_2)}$$

avec la relation, puisqu'il n'y a pas de réserve :

$(1 - D) = (1 - d_1)(1 - d_2)$

d_1 et d_2 représentant les disponibilités des composants (1) et (2).

...

5.4. Tentative de généralisation en régime limite

Le modèle markovien de fiabilité qui généralise les modèles étudiés est schématiquement le suivant :

- les caractéristiques des composants et les règles de gestion sont résumées par le processus semi-markovien de départ dont les états sont les points α, β, etc ... du système.

- la fonction de structure est une application de l'ensemble des points dans l'ensemble des états E_i du système.

- le processus d'arrivée dont les états sont les états du système résulte du processus de départ par l'intermédiaire de la fonction de structure.

Dans les deux exemples précédents le processus d'arrivée est markovien sans qu'on ait besoin de se placer en régime limite.

Mais nous allons voir qu'il s'agit là de cas particuliers et que dans le cas d'une fonction de structure quelconque le processus d'arrivée n'est plus markovien en régime quelconque mais le redevient en régime limite.

Nous resterons dans le cadre d'un processus markovien continu à un nombre fini d'états tel que :

$$\begin{cases} P_{\alpha\beta}(t) = 1 - e^{-\lambda_{\alpha t}} \\ P_{\alpha\alpha} = 0, \ \forall \alpha \end{cases}$$

De plus le processus est positivement régulier : on peut donc calculer les probabilités P^*_α pour que le système se trouve en un point donné en régime limite.

Indiquons comment généraliser à ce type de processus les résultats des paragraphes 4.2.3. et 4.2.4. relatifs aux processus de vie et de mort.

...

Supposons qu'on se trouve entre les instants t_3 et t_4 et que l'on cherche à déterminer avec quelle probabilité le système sera dans un état donné à l'instant t_4. Le dernier instant de changement d'état du système est t_3 : en $(t_3 + \varepsilon)$ l'état du composant (2) "résume" complètement son histoire puisque le composant (2) supposé "remis à neuf" vient juste de commencer une durée de fonctionnement. En $(t_3 + \varepsilon)$ le composant (1), en revanche, a un certain âge égal à $(t_2 - t_1)$ (car il est en réserve de t_2 à t_3) ; si sa loi de durée de fonctionnement n'est pas exponentielle, l'état du composant (1) ne "résume" pas parfaitement son histoire : il faut lui ajouter son âge, ce qui oblige à recenser les dates des 3 derniers changements d'état du système.

Par conséquent l'état du système, fonction des états des composants, ne suit pas un processus markovien (dont l'évolution future ne dépendrait que du dernier état et de la dernière date de changement d'état). La théorie exposée ne peut donc plus nous servir et il faut avoir recours à des processus "à mémoire".

Si la loi de durée de fonctionnement du composant (1) est exponentielle, on sait qu'elle est invariante par troncature à gauche et qu'en $(t_3 + \varepsilon)$ le composant (1) est aussi "neuf" qu'en $(t_1 + \varepsilon)$: son état "résume" alors parfaitement son histoire.

Par conséquent, en $(t_3 + \varepsilon)$ dire que (1) et (2) fonctionnent depuis t_3 "résume" parfaitement l'histoire du système.

Pour étudier les durées d'indisponibilité, plaçons-nous maintenant en $(t_2 + \varepsilon)$; l'unique loi gouvernant alors l'évolution du système est celle de la durée d'indisponibilité du composant (2) puisque (1) est passivement en réserve : (2) venant juste de débuter une durée d'indisponibilité, son état "résume" complètement l'histoire du système, quelle que soit sa loi de durée d'indisponibilité.

Les rôles de (1) et (2) pouvant être inversés, on conclut au caractère markovien de l'évolution du système,

- à condition que les lois des durées de fonctionnement de tous les composants soient exponentielles

...

- mais quelles que soient les lois des durées d'indisponibilité.

On aura cependant toujours intérêt à choisir des lois à transformées de Laplace rationnelles (voir la référence [9])pour faciliter le retour aux originales.

Les résultats précédents s'étendant immédiatement à un nombre quelconque de composants non-identiques.

En règle générale, chaque fois que l'évolution future de l'état du système ne dépend, momentanément, que de la loi d'un seul composant, cette loi peut être quelconque sans détruire le caractère markovien ; cette circonstance se produit systématiquement dans l'exemple 4.4.1. où le système ne comprend qu'un seul composant ; on a vu deux autres cas : l'exemple 4.4.2. et le modèle 5.2.

Chaque fois, au contraire, que l'évolution future immédiate du système dépend des lois de durée de 2 composants ou plus, ces lois doivent être toutes exponentielles pour conserver le caractère markovien dans le cas général ; cette hypothèse permet, en quelque sorte, la "remise à zéro des compteurs des durées" dont les origines étaient en général différentes. Le modèle 5.3. est un exemple de cette circonstance : le processus n'est markovien que si les 4 lois de durée sont exponentielles.

6.- RESUME

Dans les modèles présentés, on se donne :

- les caractéristiques de fiabilité des composants, c'est-à-dire les lois de probabilité des durées de fonctionnement et d'indisponibilité ; chaque composant peut prendre trois états : le fonctionnement, l'indisponibilité, la réserve (disponibilité sans fonctionnement)

- la manière dont l'ensemble des composants est organisé en système. Cette organisation comprend :

...

. les règles de gestion : comment sont gérés les composants lors d'une avarie ou d'une remise en état ?

. la fonction de structure : comment l'état du système dépend-il des états des composants ?

On détermine alors :

. les lois de probabilité des durées des états du système (ou du moins leurs transformées de Laplace) ; ces durées sont des temps de premier passage.

. la matrice des probabilités de passage d'un état du système à un autre.

. les probabilités limites pour que le système soit dans tel ou tel état, puisque les processus de Markov utilisés sont positivement réguliers. On en déduit diverses grandeurs moyennes dont la disponibilité du système en régime limite.

Pour effectuer ce travail, on est parti du rappel de la théorie très classique des processus de vie et de mort qui constitue l'outil adapté sur les deux hypothèses :

- tous les composants sont <u>identiques</u> (mêmes lois des durées, mêmes règles de gestion, même incidence sur la fonction de structure)

- tous les composants ont des lois de durée <u>exponentielles</u>.

Ce modèle a été perfectionné pour permettre au système de prendre trois états dont un état de disponibilité partielle. Cette amélioration a permis de constater que l'état du système ne suivait un processus markovien qu'en régime limite.

Après avoir remarqué que la théorie des processus semi-markoviens permet, dans certains cas, de lever l'hypothèse de lois toutes exponentielles, <u>cette théorie a permis d'étudier deux modèles très simples levant l'hypothèse d'identité des composants</u>.

Dans le cas d'une fonction de structure quelconque, on a constaté également que l'état du système n'avait un comportement markovien qu'en régime limite.

Enfin, on a indiqué un cas où l'on peut lever les deux hypothèses à la fois tout en continuant à utiliser l'outil markovien.

Des modèles de ce type semblent être adaptés à la détermination de la fiabilité des chaînes de production dont les composants ne sont pas identiques en général.

BIBLIOGRAPHIE

[1] FIRK, 1961

- Markov renewal processes : definitions and preliminary properties
Ann. Math. Statist., V 32, n° 4, p. 1231-1242

- Markov renewal processes with finitely many states
Ann. Math. Statist., V 32, n° 4, p. 1243-1259

[2] BARLOW et PROSCHAN

- Mathematical theory of reliability - Wiley

[3] KARLIN et Mc GREGOR, 1957

- The classification of birth and death processes
Trans. Amer. Math. Soc., V 86, p. 366-400

KARLIN et Mc GREGOR, 1959

- Coincidence properties of birth and death processes
Pacific J. Math., V 9, n°4, p. 1109-1140

[4] NEVEU, 1965

- Sur la théorie de la fiabilité
Cahiers du Centre d'Etudes et de Recherche Opérationnelle, Bruxelles

[5] COX

- Théorie du renouvellement, traduction française
Monographie Dunod

...

[6] TAKACS, 1957

- On a stochastic process concerning some waiting time problems
Teor. Veroyatnost i Primenen, V 2 , p. 92-103

[7] DOWNTON, 1966

- The reliability of multiplex systems with repair
Journal of the Royal Statistical Society, Series B, V 28, n° 3,
P. 459-476

[8] Note interne Etudes Economiques Générales d'E.D.F. - R. 926 du 23 mai 67

[9] Note interne Etudes Economiques Générales d'E.D.F. - R. 956 a, du
28 août 1967.

A. Cuoco*, R. Galvagni*, F. Leonelli**

General principles of a safety assessment through reliability analysis of the ESSOR plant

SUMMARY

For the purpose of a safety analysis of the ESSOR plant as comprehensive as possible, a probabilistic classification of both accident causes and engineered safeguards of the reactor plant has been prepared.

Accident causes have been classified within broad fault rate intervals, using as a basis both component design analysis and normal industrial practice.

Engineered safeguards have been classified according to their probability of dangerous faults.

This approach has made possible an homogeneous solution to the problem of the credibility of multiple faults.

INTRODUCTION

Faults or malfunctions in a nuclear plant could, if not prevented, evolve into accidents causing damages to the plant, to the operating staff or to the general public.

Lacking direct experience in the amount of risk deriving in such a way to the plant, to the operating staff and to the general public, analytical methods were devised to extrapolate existing experiences and criteria were set up to compare from a safety point of view different plants or different solutions.

Such a comparison requests in any case criteria of judgement of the probabilities along with methods for the appraisal of the damages of the envisaged accidents.

Therefore an ideal safety evaluation of a nuclear plant should consist for each of nuclear accident, of:

- the identification of its simple or multiple causes and the determination of associated failure rates;

* Safety and Control Division - CNEN
** ORGEL design group - EURATOM

- the identification of the interventions able to modify its evaluation and the resulting final damage and the determination of their relative dead times;
- the appraisal of the associated damages and probabilites for each accident evolution way.

From such an analysis the risk evaluation takes the form of a damage-probability spectrum.

The main difficulty in applying in a rigorous way such a method of safety evaluation is the enormous amount of information and experiences necessary in order to obtain actually consistent results in keeping with the method promises and the paid analytical effort.

Comparison and acceptability criteria cannot in any case abstract from experience on accident evolution paths and from uncertainties on extent of resulting damages and associated probabilities.

These considerations were the basis for the development of a schematic method aimed to give an hazards evaluation acceptable in the framework of the present state of experience on expected extent of damages and probability figures and to be applicable to complex and even not fully proven plant in any stage of the safety analysis.

The schematization of the method consists in using probability as a discontinuous index rather than a continuous parameter.

In order to do so, both the accidents initiating faults or malfunctions and the protective actions are divided into four probability ranges, respectively fault rate categories and relative dead time classes.

Categories and classes are related to the standard eachcomponent or protective system has or should have from the point of view of the fault or malfunction considered. The accident analysis along with the indexing procedure should be able to point out in schematic form the critical plant components that have to be examined more carefully from the point of view of accident probability or accident consequences.

The use of categories and classes related to design, construction and control standards should also give a common understanding basis for the designer, the constructor and the safety analyst.

The method, originally thought as a multiple failures credibility set of criteria, had its initial development and its first thoroughly application in the final safety analysis of the ESSOR reactor. At that stage and in view of the complexity of the analized plant it was deemed necessary to work out a simbolic system in order to analize the consequences of a number as large as possible of malfunctions, taking due account of their mutual dependence or independence and of the final resulting probability of the examined course of events. From the probability point of view, the use of criteria based on design, construction and control standards was the only solution to overcome in a rational way the lack of data based on a firm and direct experience on plants of the same type.

The method worked out had therefore the characteristics of a method of analysis of a plant as it is built.

The results of the application of the method were judged so encouraging that it was thought worthwhile further developing it in order to get it applicable through the whole design stage, when it could develop its full usefulness.

In the following both the method used in the safety analysis of the ESSOR reactor and the method at its present stage of development will be described.

ESSOR METHOD

Components and protective systems have to be classified according their reliability; such a classification is obtained using four reliability groups having from 1 to 4 increasing reliability. Groups 1 and 2 are representative of standards used in normal industry; group 3 is representative of an higher type of standards and can considered as nuclear standard; group 4 is representative of components and protective systems absolutely reliable.

Protective systems are assignedto four reliability classes according to the result of the analysis of the monitoring system, of the signal elaboreting system and of the actuating system. The protective action is classified in the class of that having lowest reliability of the three.

The criteria for class definition are as follows :

a) Class 1 — normal industrial systems from design, construction, control and maintenance points of view; possibility of having fail to danger and not revealed type of faults not minimized;

b) Class 2 — high standard industrial systems;possibility of having fail to danger type of faults not minimized,

c) Class 3 — the higher reliability is obtained by the higher degree of fail-safe or by redundancy;

d) Class 4 — intrinsic characteristics of the plant or class 3 systems redundancy.

Components are assigned to four reliability categories with regard to any specified failure way. The criteria for categories definition are quite similar to those for classes definition. In a more definite form they can be found in the description of the developed method, that is given in the following, and in Appendix 2.

The accidents analysis is carried on hypothizing the successive malfunctions or failures of the components of category 1, 2 and 3, of each subsystem of the plant and the concomitant malfunctions of the protective interventions of class 1, 2 and 3.

Particular attention must be paid to the spurious actions of protective systems which could cause accidents or increase probability of components malfunctions.

The aim of the analysis to assess the adequacy of the safety preventions and protections along any path of evolution of foreseable accidents, taking into account as far as possible also the minor accidents which could develop into serious accidents, increasing the serious accidents probability.

The fundamental criteria of such an assessment are the following:

- an accident caused by a fault or a malfunction of a component of category 4, as long as the fault or malfunction of the envisaged type is concerned, should be looked at as incredible;

- an accident caused by a fault or a malfunction of a component of category 3 should be analyzed for the consequences to the environment. In assessing such consequences the protective actions on the accident path should be evaluated both for capability and reliability. As long as the reliability is concerned, it should be looked at missing intervention of protective systems of class 4 or at missing intervention of redundant and independent class 3 protective systems as incredible. If the independent class 3 protective systems are not equivalent from the point of view of damage reduction, it is hypothesized that the active one is the less effective on damage reduction;

- an accident caused by a fault or a malfunction of a component of category 2 should be analyzed for the consequences both to the environment and to the operating staff. In assessing the consequences to the environment the criteria should be those aforementioned but the resulting damages should be of one order of magnitude less than those arising from the most serious of category 3 accidents.
In assessing the consequences to the operating staff full advantage can be taken of the protective actions of class 3 or of equivalent redundance of class 2 (redundance from the reliability point of view, with effectiveness of the less effective on damage riduction).

The reliability assessment of the ESSOR reactor protective systems is carried out for each of the three fo lowing main plant systems:

1) Nuclear and cooling system

2) Pressure and fire protections and containment system

3) Fuel handling system

The components are then classified into categories and components categories and protective actions classes are listed for each of the following subsystems of each of the main system

1. Nuclear and cooling system

- Reactor
- Driver zone cooling system
- Moderator zone cooling system
- Experimental organic zone cooling system
- Experimental light water zone cooling system
- Electric power sypply system

2) Pressure and fire protections and containment system

- Containment system
- Pressure and fire protective systems

3) Fuel handling system

- Charging and discharging machines
- Handling stations system

An example of the classification of the protective actions and components of the Driver zone cooling system is given in Appendix 1.

DEVELOPMENT OF THE METHOD

The aim of the extension and of the reorganization of the method is to keep the designer fully informed of the safety evaluation criteria, setting those in a form as precise as possible at the present stage.

The method should therefore supply a working tool for the definition of design solutions which are equivalent from a safety standpoint.

The procedure to be followed for the assessment is divided into the following steps:

a) Listing of all foreseable accidents with the fault or malfunction of the components causing them;

b) Classification of accidents causes into categories according to failure rates criteria.
If a specific failure rate value is not available, the category is defined according to design criteria, to contruction, test and control standards and to type and periodicity of controls and maintenance during operation, taking into account their bearing on the specific component failure considered;

c) Division into classes of protective systems, capable of preventing or limiting the listed accidents; the classification should be made according to relative dead time criteria.
If the relative dead time is not available the class is defined according to design criteria, construction test standards and to type and periodicity of controls and maintenance during operation;

d) Evaluation of the risks associated with the listed accidents, taking into account causes categories and effective protective actions classes.

a) Accidents identification

The accidents identification and the evaluation of their consequences are carried out according to traditional safety analysis criteria and methods.
But in order to have a meaningful probabilistic assessment it is necessary to analyse in a fully systematic way all foreseable accidents and the effects on their consequences of each protective system which can modify the accident evolution.
During the application of the method at the design stage it is necessary to re-examine continuosly both the classes and the consequences of accidents as the components and the protective systems gain a better definition and as one makes a selection among a number of possible equivalent solutions.

b) Accidents causes classification

The aim of the components categorization is to put together components having comparable reliability in front of the examined type of fault or malfunction. Such a collection should be based as far as possible on practical industrial criteria.

At the present stage, it is proposed to use in the components classification four categories, characterized by increasing reliability:

- Cat. 1: normal industrial - type reliability
- Cat. 2: high industrial-type reliability
- Cat. 3: aeronautics-type reliability
- Cat. 4: almost absolute reliability

Cat. 1

This is among the four the category whose boundaries are most difficult to define precisely and probably the largest one.

All industrial components both those which have not been and those which cannot be subjected to standard specifications, to standard tests or to effective inspections and maintenance, are classified into cat. 1. Components that can malfunction as consequence of bad maintenance during plant operation without possibility of effective and timely control are also classified into cat. 1.

From a safety point of view such kind of components should be demonstrated not to cause nuclear accidents.

Cat. 2

Components classified into this category should have a high industrial standard with respect to the examined functional requirement. Characterizing components are those which in the working conditions satisfy official normal industrial type standards both as fabrication and tests and as periodical inspections are concerned. Components in cat. 2 are also those which are used as a consequence of a selection derived from a significant experience on their behaviour in the working conditions. In any case missing official tests and control standards, appropriate standards must be defined and adopted. Components which could have better classification but which are liable to malfunction as consequence of bad maintenance are also classified in cat. 2 if not protected against by appropriate alarms or interventions.

Cat. 3

Components classified into this category should satisfy higher standards than normal industrial official standards.

The larger safety margins could result from:

- working conditions sensibly less stringent than the corresponding ones admitted by normal industrial official standards

- preventive maintenance (e.g. of aeronautics type)

If there are multiple components of category 2, which are independent, separately proof-tested and singly assuring the complete requested function, loss of such a function can be classifed in category 3.

Cat. 4

This category is typical of functions of almost absolute reliability. It is referred to the expected rate of a specific and well defined fault type of the component, rather than to the component failure rate. The almost absolute reliability can be obtained by:

- redundancy of components of category 3, which are independent, separately proof tested and which can independently assure the complete requested function;

- demonstrated and safe impossibility in the particular working conditions of the happening of the type of fault; unless this may develop as an evolution of faults of the lower categories. A further condition is that the lower category fault be detected in due time, so to avoid a further fault evolution.

On the basis of the definition of reliability, the criteria is proposed that, from a safety standpoint, the happening of faults or malfunctions of category 4 be considered incredible.

Protective systems classification criteria

A classification of components into four categories, with respect to their possible malfunctions, should allow the subdivision of the causes which could initiate accidents into four classes, homogeneous from an extimated rate standpoint.

In order to continue the analysis of damage probability it is necessary to evaluate safety protective actions.

In any of the protective systems we can identify a detection system, which can pick out abnormal situations, a processing system, which can transform a detection into a logic decision, an actuating system which actuates the logic decision in such a way as to correct or contain the evolution of the abnormal situation.

The detector, the processing system and the actuator can be classified independently on the basis of the respective relative dead time. In doing so, a reliability class is attributed to any one of them. The entire protective action has a characteristic reliability class which is the lowest of the three.

In the first stage of the setting up of reliability criteria the classification of detectors, processing systems and actuators can be made by arranging them according to practical criteria, using as far as possible industrial-type concepts in more or less homogeneous reliability intervals.

At the present stage, we propose to use for them too a classification into four classes, defined as follows:

- Class 1: normal industrial-type reliability
- Class 2: high industrial-type reliability
- Class 3: aeronautics-type reliability
- Class 4: almost absolute reliability

Class 1

Class 1 is typical of those systems in whose design has not been deemed appropriate to use particular design precautions and particular choice of components in order to drastically reduce the relative dead time. This class has the distinctive features of a normal industrial standard, has no fault detection system, is subject to maintenance after the fault has been detected; this detection is carried out at time intervals suggested by normal use. This class includes all those interventions which without following any particular procedure or initiating alarms, could either be by-passed or be made inoperative by wrong maintenance. Furthermore, this class includes operator interventions which should be carried out in emergency conditions and which are not univocally defined.

Class 2

Class 2 has the distinctive features of a high industrial standard, is not supposed to have a high fail-safe degree, and is subjected to very attentive and frequent maintenance. This class includes all those interventions which could be by-passed during operation with particular procedures which involve multiple responsibilities; it does include as well those interventions which could be made inoperative by wrong maintenance and which, even though in this condition do initiate control alarms, do not initiate an automatic exclusion or fail-safe action. It does also include operator interventions which should

carried out in times of the order of several minutes on the basis of written orders.

Class 3

Class 3 is typical of those systems where not only a particular choice of components and preventive maintenance, but also redundancy, an high degree of fail-safe and autocheck system, reduce the relative dead time to values which can not be obtained by an industrial standard, even by a high one.

These systems are typical of nuclear plants (e.g. high flux trip systems, etc); they have been defined "aeronautics standard" only to point out the results which can be obtained trough an analysis of failure rates, preventive maintenance, an appropriate testing system, and the importance of obtaining such results.

A common need of these systems is that they should not be by-passed in normal plant operation, but only during shut-downs, to program particular operating cycles.

Class 4

Class 4 is typical of those systems which use, in order to obtain protective actions, or well known intrinsic characteristics of the nuclear reactor or of the plant itself or are obtained through redundancy of independent class 3 systems, or which have so advanced and well defined fail-safe or autocheck characteristics to be equivalent from a relative dead time point of view to redundancy of independent class 3 systems.

Speaking about the whole classification system, it can be of interest to note that if there are any uncertainties deriving from a lack of specific experience on a given system, on its effective working conditions on its independence from the systems with which it does redundate a degradation of the reliability class of the action to which the system belongs is mandatory.

On the other hand, redundancy, testing methods at meaningful time intervals and a counterchecked preventive maintenance can upgrade the reliability class.

A number of examples of component classification into categories and protective systems into classes are given in Appendix 2.

Risk evaluation

By definition, risk is the product of damage and its probability Damage evaluation is performed through an analysis of the typical accidents with the usual approximation.

Probability evaluation can be performed for any typical accident taking into account the category of the accident cause and the classes of the associated interventions. It is thus possibile to reach a symbolic definition of the probability interval of the damage. This technique lends itself to an elaboration of acceptance criteria based either on the multiple failure concept(MCA - type criteria) or on the definition of a tolerance interval in the damage vs. probability field.

DEFINITIONS

1. Equivalent solution: technical solutions through which it is possible to obtain values of risk (damage times probability) of the same order of magnitude.

2. Component: system which has a complete and well defined physical function with respect to the type of accident under consideration.

3. Type of accident: accident defined through its nature, evolution in time and consequences, taking under examination capability and effectiveness of single and multiple interventions which could prevent or limit it.

A d d e n d u m I

APPLICATION EXAMPLE OF THE METHOD ON THE ESSOR REACTOR

ACCIDENT ANALYSIS ON THE DRIVER ZONE COOLING CIRCUITS (Fig. 1)

In table 5 are listed all causes of accidents on the DRIVER ZONE cooling. To any component failure will be associated the relative category, following the criteria already explained before.

In table 4 are listed and classified all protective actions, designed to prevent or reduce the accidents of loss of cooling of the driver elements.

The parts of the protective systems are classified in the following tables :

- Table 1 : monitoring systems
- Table 2 : elaborating systems
- Table 3 : actuators.

With the aim to keep the example simple, it will not be extended to other protection systems as f.e.

- emergency cooling system
- containment, etc.

We have limited the analysis to the most severe accidents of the family A.

LOSS OF FLOW ACCIDENTS IN THE PRIMARY CIRCUIT

The most severe accident of family A listed in table 5 is : MA_4. "All primary pumps stopped and no auxiliary pumps started", which

./..

may be regarded as well as the maximum accident of this family.

Safety Interventions linked to MA4

a) Power setback or control rod run-down

1) one primary pump stopped	- 3 x K4
2) two primary pumps stopped	- K5
3) CORE outlet low flow	- K3
4) high outlet temperature and low outlet flow for each channel	- 16 x K1
5) CORE outlet high temperature	- K2

b) Scram

1) three primary pumps stopped	- A6
2) CORE outlet low flow	- A3
3) high outlet temperature and low outlet flow for each channel	- 16 x A1
4) CORE outlet high temperature	- A2

The probability of a reactor shut-down is represented by the independant interventions : 1 . C2 + 2 . C3.

These protective actions and their relative class of reliability assure that the reactor will be shut-down following the failure MA4.

Evalutation of the accidents

Under assumption that no protective action is forseen for accident MA4 and considering only the inertion of the pumps fly wheels, with the reactor at nominal power, the temperature of driver zone hot spot will encrease with 2.5°C/sec and the coolant outlet temperature with 0,8°C/sec.

Given the reliability of the protective interventions, and the slow ness of the temperature increase, the reactor will be shut down before any fuel damage has occurred.

./..

After a complete stop of all primary pumps, natural circulation will occur with the improbable possibilities of nucleate boiling during the first minutes.

Thus the accident will have no radiological consequences while no fuel damage will occur.

Table 1 : CLASS OF MONITORING SYSTEMS

Monitoring system	Symbol	Class	Notes
Outlet channel temperature (16 channels)	T1	2	Monitored for minimum reading
Outlet core temperature	T2	3	2/16 combination of T1
Outlet channel flow	F1	2	Monitored for minimum reading
Outlet core flow	F2	3	2/16 combination of F1
Expansion tank pressure	P1	3	2/3 monitored pressure switches
Expansion tank level	L1	2	dP-cell monitored for minimum reading
Primary pump stop signal	B1	2	Closed to open contact on pump braker
Secondary pump stop signal	B2	2	Idem
Moderator level	L2	3	2/3 level switches

a/oo

a/xx

Table 2 : CLASS OF ELABORATING SYSTEM

Elaborating System	Symbol	Class	Notes
Scram logic system	SS-1n	3	
Power set-back system	SS-2	2	
Control rod run-down system	SS-3	2	
Pressure reduction system	SS-5	2	
Auxiliary pumps starting system	SS-6	2	2/3 pumps
Feeding pumps starting system	SS-7	2	1/2 pumps
Primary pumps stopping system	SS-8	2	

Table 3 : CLASS OF ACTUATORS

Actuator	Symbol	Class	Notes
Safety rods group 1 or 2	R-1	3	The safety rods are divided into 2 independent groups (drop of 2/4 has class 4)
Control rods	R-2	2	
Motor driven valves	V-1.n	2	
Feeding pumps start	V-2	2	1/2
Auxiliary pumps start	V-3	2	2/3
Primary pumps brakers	V-4	2	

Protective Action	Symbol	M. S. Class	E. S. Class	Ac. Class	Class
Scram	A				
High outlet temperature and low outlet flow for each channel	A-1	T1.F1/2	SS-1.1/3	R-1/3	2
Core outlet high temperature	A-2	T2 /3	SS-1.2/3	R-1/3	3
Core outlet low flow	A-3	F2 /3	SS-1.3/3	R-1/3	3
Expansion tank high pressure	A-4	P1 /3	SS-1.4/3	R-1/3	3
Expansion tank low level and channel outlet low flow	A-5	L1.F1/2	SS-1.5/3	R-1/3	2
3 primary pumps stopped	A-6	B1 /2	SS-1.6/3	R-1/3	2
3 secondary pumps stopped	A-7	B2 /2	SS-1.7/3	R-1/3	2
Moderator high level	A-8	L2 /3	SS-1.8/3	R-1/3	3
Run down and set back	K				
High outlet temperature and low outlet flow for each channel	K-1	T1.F1/2	SS-2 /2	R-2/2	2
Core outlet high temperature	K-2	T2 /3	SS-2 /2	R-2/2	2
Core outlet low flow	K-3	F2 /3	SS-2 /2	R-2/2	2
Primary pumps stopped 1/3	K-4	B1 /2	SS-2 /2	R-2/2	2
Primary pumps stopped 2/3	K-5	B1 /2	SS-3 /2	R-2/2	2
Secondary pumps stopped 3/4	K-6	B2 /2	SS-3 /2	R-2/2	2

./..

Protective action	Symbol	N. S. Class	E. S. Class	Ac. Class	Class
Depressurisation of the Expansion tank	D				
Expansion tank low level and moderator high level	D-1	L1.L2/2	SS-5/2	V-1.1/2	2
Expansion tank low level and channel outlet flow	D-2	L1.F1/2	SS-5/2	V-1.1/2	2
Primary pumps deenergize	S				
Expansion tank low level and moderator high level	S-1	L1.L2/2	SS-8/8	V-4 /2	2
Expansion tank low level and channel outlet low flow	S-2	L1.F1/2	SS-8/2	V-4 /2	2
Feeding pumps start	E				
Expansion tank low level	E-1	L1 /2	SS-7/2	V-2/ 2	2
Expansion tank minimum level	E-2	L1 /2	SS-7/2	V-2 /2	2
Auxiliary pumps start	H				
Expansion tank low level and channel outlet low flow	H-1	L1.F1/2	SS-6/2	V-3 /3	2
Expansion tank low level and moderator high level	H-2	L1.L2/2	SS-6/2	V-3 /3	2

Table 5/1 : CATEGORY OF CAUSES OF ACCIDENT

Causes of accident	Symbol	Category	Notes
A - Loss of flow			
- Primary pumps stopped	MA1	1	
- 2 primary pumps stopped	MA2	2	
- 3 primary pumps stopped	MA3	2	
- 3 primary pumps stopped and no auxiliary pump started	MA4	3	
- Feeding pump not stopped	MA5	2	
- Feeding pump not started	MA6	2	
- Primary circuit valve accidentally closed	MA7	2	
- Primary circuit completely blocked	MA8	4	
B - Loss of coolant			
- Leakage from primary circuit to reactor tank	MB1	2	
- Pump sealing leakage	MB2	2	
- Valve sealing leakage	MB3	2	
- G.A.A.A. joint leakage	MB4	2	
- Flange leakage	MB5	3	Double O ring and interface monitored
- Instrumentation pick-up leakage	MB6	2	
- Leakage through B.S.D.	MB7	1	
- Loss of coolant due to an accident heat exchanger dumping valve opening	MB8	3	
- Expansion tank overflow valve opening	MB9	2	
- Expansion tank depressurization valve opening	MB10	2	
- Instrumentation pick-up breakage	MB11	3	
- Heat exchanger breakage	MB12	2	
- Primary piping breakage	MB13	3	
- Inlet primary circuit collector breakage	MB14	3	
- Outlet primary circuit collector breakage	MB15	3	

Causes of accident	Symbol	Category	Notes
- Channel inlet piping breakage	MB16	3	
- Channel outlet piping breakage	MB17	3	
C - Loss of cooling			
- Secondary pump stopped			
2/4	MC1	1	
3/4	MC2	2	
4/4	MC3	2	
- Secondary pumps stopped without emergency system started	MC4	3	
- Secondary coolant of heat exchanger isolation	MC5	2	
- Drainage of secondary coolant from heat exchanger	MC6	2	
- Losses of secondary coolant through piping breakage	MC7	2	

A d d e n d u m I I

ACCIDENT CATEGORIES AND CLASSES OF PROTECTIVE SYSTEMS

I) EXAMPLES OF ACCIDENT CAUSES CATEGORIES

A) Components, causes of accidents of the first category (G1)

a) Mechanical components

Bearings	Normal, not monitored and not subjected to preventive maintenance (at intervals defined by endurance tests)
Seals	Seals on moving systems, without leak detection, and not subjected to preventive maintenance (at intervals defined by endurance tests)
Valves	Normal valves, operating under environmental conditions different from commissioning conditions, and without preventive maintenance
Static components	Tubing, expansion joints, supports, not specially tested by commissioning institutions (AMCC-T.U.V. etc.) operating under not exactly known conditions, and not subjected to periodic inspection or preventive maintenance
Control valves	Operating under stressed conditions and not subjected to inspection or preventive maintenance

b) Electrical components

Relais	Operating under stressed conditions and not subjected to inspection and preventive maintenance
Circuit breakers	Operating under stressed conditions, and not installed in closed cabinets

Electric cables	Unarmoured and unprotected cables installed in damaging environment
Electronic equipment	Not subjected to inspection or preventive maintenance
Electric motors	Not protected, operating under damaging environmental conditions and under overload - frequent start and stop under load.

c) Operator interventions

- Positioning of actuators, not equiped with out of range alarms
- Manual setpoint adjustments
- Direct interference on interblock by-passes.

B) Components, causes or accidents of the 2nd category (G2)

a) Mechanical components

Bearings	Special bearings operating according commissioning conditions monitored for temperature and lubrification, and equiped with alarm trips permitting in time corrective intervention by the operator
Seals	Seals on moving parts operating according commissioning specification monitored for leaks and equiped with alarm trip permitting corrective intervention by the operator
Valves (check and control valves)	Quality valves, operating according commissioning specification, subjected to inspection and preventive maintenance
Safety valves	Safety valves dimensioned and designed according the rules of national safety institutions (ASCC - T.U.V. etc.) or equivalent

b) Electric components

Relais	Quality relais in base current, installed in cabinets or at least in non aggressive environmental conditions, and subjected to inspection and preventive maintenance
Circuit breakers	Operating in non aggressive environment and installed in closed cabinets
Electronic circuits	Subjected to preventive maintenance
Electric motors	Operating in non aggressive environment, largely overdimensioned and not subjected to frequent starts and stops under load

c) Operator interventions

- Positioning of actuators, equiped with out of range alarms
- Setpoint adjustment or by-pass consent with key interblock

C) Component failures, causes of third category accidents (G3)

a) Mechanical components

- Gripping of lubrificated and monitored bearings, when bearings are at least of the 2nd category
- Major rupture of primary main tubings when these tubings are at least 25%-30% overdesigned with respect to the effective operation conditions, taking into account thermal and vibrational stresses
- Double seals of the second category type, with monitored interspace.

b) Electrical components

Cables	Short circuit on armoured or protected cables, installed in non aggressive environments

Distribution busbars	Short circuit on busbars installed in closed cabinets

D) Failures, causes of fourth category accidents (G4)

a) Accidents due to mechanical failures

- Contemporaneous rupture of a double walled tubing, each containment independant and of category 3 and each continuously monitored
- Major rupture of the reactor vessel which is designed and commissioned according nuclear standards and regularly inspected

II) CLASSES OF PROTECTIVE SYSTEMS

The reliability of a control system or of a measuring channel depends nearly exclusively on the design criterious and on the working conditions of the various elementary components.

The following elements are taken into insideration to judge the realiability :

1) Type of failure : - fail-safe
- fail to danger signalized or not signalized

2) Possibility and procedures of switching off

3) Possibilities and conditions of inspection and verification.

A) Systems of class 1

Protective systems of class 1 do not require a reliability evaluation

B) Systems of class 2

All components of a protective system of class 2 must be of a proven type and adequately tested under effective operation conditions

./..

a) Detectors and measurements

- Protected thermocouples (well mounted) of an ample life time under the operation conditions, and with preventive substitution
- Instruments of good industrial standard, tested under effective operation conditions, subjected to preventive maintenance

b) Elaboration systems and control circuits

- Simple solid state logic, or relais without base current, equiped with a control system "a posteriori"
- Relais logic with base current, subjected to preventive maintenance and equiped with a failure alarm

All logic of class 2 should be installed in closed cabinets.

c) Actuators

- Electrical motors operating in non aggressive environment and of a proven type with regards the effective operation conditions
- Circuits breakers, operating in non aggressive environment and installed in closed cabinets
- Valves, control valves or remote controlled check valves, subjected to praventive maintenance

C) Protective systems of class 3

For these systems a reduction of the relative dead time to values not regularly obtainable with common industrial standards may be realized with the following rules :

1. The use of overdesigned components (resistor, diode, etc. at 60%)
2. The use of "fail-safe" logic or the addition of an autocontrol system which translates non fail-safe failures in fail-safe ones
3. Redundancy - beside an increased reliability, redundancy in general permits maintenance during operation

4. Preventive maintenance by which single components will be submitted at 70% of their guaranteed life time.

Rule 4 may be applied when it is not possible to design according to rule 2.

a) Measuring system

Constituted of redundant number of measuring channels of good industrial standard, equiped with a continuous autocontrol system. In case of failure, the autocontrol system triggers an intervention equivalent to the level trip. Beside that, the system must be equiped with a common alarm to indicate any channel failure or any alarm trip.

b) Elaboration system

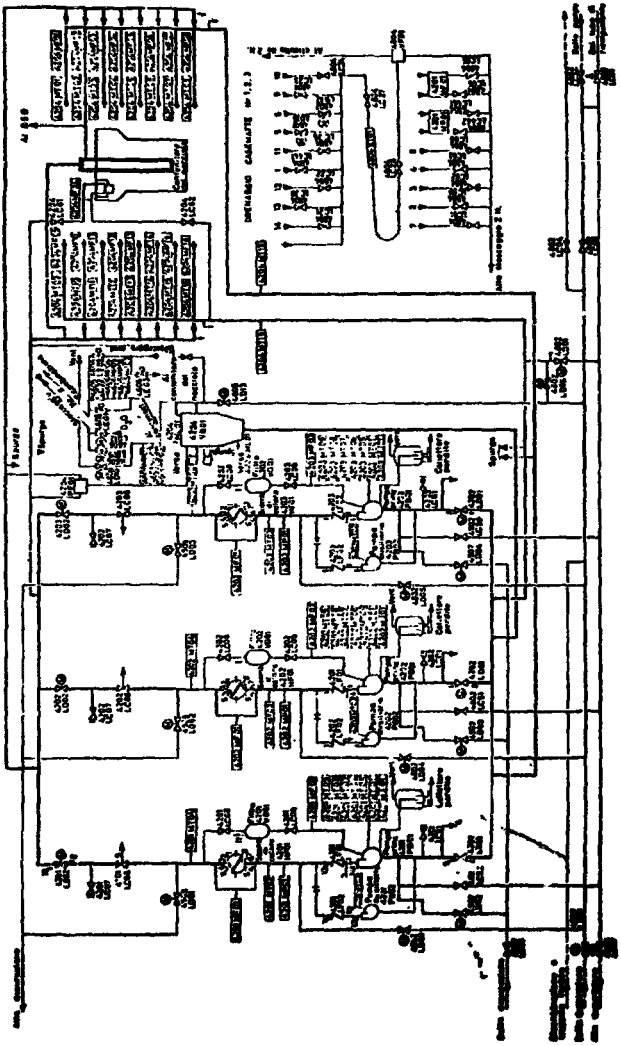
The logic and control system should be with base current, and equiped with an autocontrol system, which translates any non fail-safe failure in a fail-safe one.
The logic circuits associated to more than one intervention of class 3 beside being extremely reliable, eventually has to be duplicated in order not to impair the degree of redundancy of the interventions. The autocontrol system should test all duplicated lines separately and independantly.

c) Actuators

The actuators have to be fail-safe as far as possible and of the base current type.
In a detail study all possible failure should be examined, passive as well as active. From this detailed study can be deduced whether a redundancy of the actuator is necessary.

FIG. 1

CIRCUITO P_{22} ZONA NUTRICE



AGENCE EUROPEENNE POUR L'ENERGIE NUCLEAIRE
COMITE DES TECHNIQUES DE SECURITE DES REACTEURS

Réunion de spécialistes en matière de fiabilité des composants et des systèmes mécaniques destinés à assurer la sécurité des réacteurs

---

QUELQUES REMARQUES SUR LA FIABILITE EN MECANIQUE

par

C. MICHEL*

* Société B RTIN - Boîte Postale n° 3 - 78 PLAISIR.

1 - INTRODUCTION

Le bref exposé qui va suivre est le résumé, d'une part des remarques que nous avons pu faire au cours de l'exercice de nos activités quotidiennes qui s'exercent dans des domaines comme l'aérodynamique, l'électronique, la thermique, l'automatique, et d'autre part des analyses bibliographiques que nous faisons d'une façon continue et au sujet desquelles on trouvera en annexe quelques références.

De tout temps les constructeurs ont cherché à conférer à leurs fabrications une sûreté de fonctionnement satisfaisante pour les utilisateurs, mais pendant très longtemps cette sûreté de fonctionnement déterminée par des essais de laboratoire où les résultats de fonctionnement en clientèle ne présentait qu'un caractère qualitatif ou si une valeur quantitative en était donnée aucun traitement mathématique ne permettait d'en généraliser la signification.

- C'est depuis la seconde guerre mondiale qu'est apparu le besoin de quantifier la sûreté de fonctionnement. Ce besoin a donné naissance à une discipline nouvelle que nous appelons en francais fiabilité et que les anglais nomment reliability.

Bien qu'inséparable de la notion de conception de systèmes, la fiabilité s'en distingue par les connaissances mathématiques et statistiques qu'elle requiert. C'est une branche de la recherche opérationnelle.

Parmi les nombreuses causes qui sont à l'origine du besoin de quantifier la sûreté de fonctionnement nous retiendrons :

- la naissance de techniques nouvelles dont la rapidité d'évolution ne permet pas aux techniciens de se référer à des résultats d'expériences passées d'où la nécessité de posséder des méthodes qui permettent de

prédire, puis d'améliorer la fiabilité de systèmes nouveaux.

- la complexité croissante des systèmes ne permettant plus d'estimer les sûretés de fonctionnement grâce à l'unique bon sens

- des performances de systèmes toujours plus élevées, impliquant d'utiliser les matériaux aux limites de leurs possibilités ce qui exclue l'utilisation de larges coefficients de sécurité ou d'ignorance.

- une concurrence économique très vive obligeant l'industrie à optimaliser ses choix pour réduire les coûts, à organiser rationnellement la maintenance, à réduire les stocks, les temps d'immobilisation des machines, etc... d'où la naissance de nombreux concepts dérivés de celui de fiabilité, telles la disponibilité, la pertinence, etc...

- la conception d'installation ou de machines dont la défaillance peut entraîner la mort (avions, fusées, réacteur nucléaire, etc...) avec en plus des implications financières et psychologiques.

Avant d'aller plus avant, nous essaierons de classer les systèmes que l'on a composé généralement en sous systèmes ou sous ensembles eux-mêmes décomposés en composants ou pièces élémentaires.

2 - DIFFERENTS TYPES DE SYSTEMES

Nous proposons de distinguer deux familles de systèmes :

les systèmes structuraux et les systèmes informationnels

Les premiers sont ceux dont la fonction principale consiste à transmettre des efforts ou assurer des positionnements tels la poutre d'un pont, la membrane d'une aile d'avion ou le tube d'un télescope.

La fonction principale des seconds est de transmettre des informations qui peuvent être : une force, un débit, une pression, un déplacement, etc... On rangera dans cette famille les systèmes électriques et électroniques et aussi les systèmes mécaniques comme les asservissements hydrauliques par exemple.

Ces derniers systèmes sont composés d'organes de structures qui transmettent des efforts, le corps d'une vanne par exemple, et d'organes de liaison comme les joints d'étanchéité.

Le type de pannes subies par les systèmes pouvant, d'une part caractériser ces systèmes et, d'autre part définir les méthodes de calcul de la fiabilité à utiliser, nous rappellerons, dans le paragraphe suivant, des définitions relatives aux défaillances telles qu'elles sont exprimées par Messieurs CHAPOUILLE et DE PAZZIS dans la référence B 6 page 8.

3 - DEFINITION DES DEFAILLANCES

Défaillance : Fin de l'aptitude d'un dispositif à accomplir sa fonction requise.

Défaillance soudaine : Défaillance qui n'aurait pas pu être prévue par un examen antérieur des caractéristiques.

Défaillance progressive : Défaillance qui aurait pu être prévue par un examen antérieur des caractéristiques.

Défaillance partielle : Défaillance résultant de déviations d'une ou des caractéristiques au-delà des limites spécifiées mais telles qu'elles n'entraînent pas une disparition complète de la fonction requise.

Défaillance complète : Défaillance résultant de déviations d'une ou des caractéristiques, telles qu'elles entraînent une disparition de la fonction requise. Les limites correspondant à cette catégorie sont des limites spéciales spécifiées dans ce but.

Défaillance cataleptique : Défaillance qui est à la fois soudaine et complète.

Défaillance par dégradation : Défaillance qui est à la fois progressive et partielle.

Défaillance d'exploitation : Défaillance causée par le non-respect des règles d'exploitation spécifiées ou par des influences extérieures dépassant les limites prévues dans les conditions d'exploitation du dispositif considéré.

4 - METHODES GENERALES UTILISEES EN ELECTRONIQUE

Les études de fiabilité se sont considérablement développées avec l'essor de l'électronique et cela pour trois raisons principales :

- les systèmes électroniques sont constitués de centaines de composants et en raison de la complexité qui en découle, leur fiabilité ne peut être déterminée que grâce à des méthodes très élaborées.

- les composants électroniques ont généralement un taux de panne constant c'est-à-dire une loi de survie exponentielle, forme mathématique qui ne conduit pas à des calculs trop inextricables.

- le grand nombre de composants qui confère une extrême complexité aux systèmes, présente l'avantage de permettre des estimations statistiques précises en raison même de ces grands effectifs.

Nous avons vu dans les définitions que l'on distinguait les défaillances soudaines et les défaillances progressives.

A ces deux types de défaillance on peut faire correspondre deux familles de calcul.

Dans le premier cas on décompose le système en sous systèmes ou modules et on représente les liens entre ces derniers du point de vue de la fiabilité par un schéma dit bloc-diagramme de fiabilité auquel on applique les règles du calcul des probabilités. Pour améliorer la fiabilité d'un système, on peut, d'une part choisir des composants plus fiables ou les relier suivant un schéma plus sûr c'est-à-dire en utilisant par exemple la redondance qu'elle soit active ou de substitution.

Dans le cas des défaillances progressives, l'étude de fiabilité consiste, à partir du diagramme fonctionnel , à définir comment varient les paramètres de sortie en fonction de la variation des paramètres d'entrée, ce que les américains appellent PVA ou parametre value analysis.

On peut classer les méthodes de PV A en deux familles suivant que l'on ne fait pas ou au contraire que l'on fait intervenir la distribution probabiliste des paramètres.

L'analyse de la sensibilité et l'étude du cas le plus défavorable (worst case) se présentent dans le premier cas, l'analyse des moments, la méthode de convolution et les méthodes de Monte Carlo apparaissent dans le second.

1 - Etude de sensibilité

La sensibilité d'un système caractérise la variation d'un ou des paramètres Y_j de sortie en fonction de la variation d'un ou des paramètres d'entrée X_i. Elle correspond à la notion d'élasticité en économie et peut être définie mathématiquement par :

$$S_{X_i}^{Y_j} = \frac{\Delta y_j / Y_j}{\Delta x_i / X_i}$$

Son étude permet de déterminer les paramètres dont la dérive influencera le plus les performances du système.

Dans ce type d'étude, les variations des paramètres d'entrée sont faibles. Si au contraire on donne à ces paramètres des amplitudes de variation extrêmes on fait une analyse du cas le plus défavorable (ou worst case analysis) qui correspond à la vérification d'un fonctionnement satisfaisant du système au cas où le principe bien connu de l'ennui maximum s'appliquerait.

2 - Lorsque l'on désire connaître la probabilité de voir la valeur des paramètres de sortie dépasser ses tolérances, on fait appel à la méthode dite des moments, nommée ici car elle porte sur les deux premiers moments de la distribution des paramètres d'entrée, c'est-à-dire, la moyenne et la variance, cette méthode est aussi dénommée méthode de la propagation de la variance. Elle suppose des distributions normales et des paramètres de sortie variant linéairement en fonction des paramètres d'entrée.

La méthode de convolution n'implique pas une distribution normale des paramètres d'entrée, elle a pour base l'hypothèse que la variation totale d'un paramètre de sortie est la somme des variations partielles de ce même paramètre de sortie, causées par chacun des paramètres d'entrée.

Dans le cas très général où les distributions sont quelconques et les systèmes très compliqués on peut faire appel aux méthodes de Monte Carlo qui ont pour base le théorème de Glivenko- Cantelli et correspondent à une véritable expérimentation sur ordinateur. Elles conduisent souvent à des temps de calcul élevés et à des dépassements de capacité. Elles sont par contre très générales.

Enfin, une méthode générale qualitative consiste à analyser les causes et les effets d'un certain nombre de défaillances de composants (failures modes and effects analysis).

5 - FIABILITE MECANIQUE

Après avoir brièvement rappelé les méthodes utilisées pour les calculs de fiabilité en électronique, nous aborderons le cas de la fiabilité en mécanique.

Nous essaierons d'abord de distinguer en quoi la fiabilité mécanique présente un caractère original, nous énumérerons ensuite les méthodes utilisables dans les études de fiabilité mécanique, nous conclurons enfin en suggérant les travaux qu'il nous semble souhaitable d'entreprendre pour faire progresser la fiabilité mécanique.

La particularité essentielle des systèmes mécaniques réside en la difficulté d'obtenir des résultats statistiques significatifs. Cette carence est due au fait que les systèmes mécaniques sont généralement construits en nombre restreint et que de plus leurs conditions d'utilisation et de maintenance sont extrêmement variables. Cette difficulté de faire de la statistique en fiabilité mécanique apparaît bien si l'on compare la définition de la fiabilité donnée par les électroniciens à celle énoncée par l'Académie des Sciences et qui se veut plus générale.

Définition en électronique.-
"Probabilité qu'un dispositif accomplisse une fonction requise dans des conditions d'utilisation et pour une période de temps déterminés".

Définition de l'Académie.-
"Grandeur caractérisant la sécurité de fonctionnement, ou mesure de la probabilité de fonctionnement d'un appareillage selon des normes prescrites".

Outre cette différence formelle, notons que la fiabilité des composants mécaniques dépend comme les composants électroniques de l'environnement (température, vibrations) mais est de plus sensible à l'interaction des

pièces voisines et des caractéristiques de leur liaison.

Ainsi on peut constater une forte différence entre la fiabilité intrinsèque d'un composant telle qu'elle est déterminée au laboratoire et la fiabilité opérationnelle dudit composant. Un exemple significatif est celui des roulements à billes dont la durée de vie peut être singulièrement écourtée par un montage inadéquat.

Une autre particularité de la fiabilité des systèmes mécaniques est que ces derniers sont réparables, ce qui a des conséquences, en particulier pour les systèmes informationnels, que nous évoquerons plus loin.

Abordons maintenant les différentes étapes de la détermination de la fiabilité mécanique. Rappelons d'abord que la fiabilité se prédit au stade du projet, s'estime au niveau du prototype et s'évalue au niveau de la série.

- Fiabilité des organes

.- Estimation de la fiabilité

Lorsque les composants sont très nombreux, les méthodes générales utilisées en électronique et en contrôle de qualité s'appliquent bien pour estimer la fiabilité intrinsèque. Le meilleur exemple est celui des roulements à billes.

Il peut aussi être intéressant, lorsque l'on a affaire à une lignée d'organes semblables, de déterminer, au laboratoire, sur de grands effectifs, la famille à laquelle appartient la loi de fiabilité. Des essais en nombre réduit sur l'organe particulier qui nous intéresse suffiront ensuite à déterminer les paramètres de la loi dans ce cas particulier. Nous pensons ici tout spécialement au cas où la loi de Weibull s'applique, l'on sait qu'elle se représente par une droite avec les coordonnées du diagramme d'Alan Plait, ce qui réduit théoriquement à deux les essais nécessaires.

.- Prédiction de la fiabilité d'un organe

L'on sait que le nombre des corps simples est de l'ordre de 10^2, le nombre des organes de l'ordre de 10^3 et le nombre des ensembles de l'ordre de 10^5. Partant de cette constatation, il semble plus simple d'aborder l'étude de la fiabilité au niveau des matériaux constituants plutôt qu'au niveau des ensembles.

Pour ce faire, on est conduit à comparer la position respective de la loi de distribution des charges à la loi de distribution de la contrainte admissible pour le matériau.

Ce point de vue est original car d'ordinaire on se contente de comparer une valeur moyenne de contrainte à une valeur moyenne de la résistance du matériau en ayant pris la précaution d'introduire un coefficient de sécurité ou d'ignorance qui permet de maintenir celle-ci inférieure à celle-là.

Cette méthode présente un aspect statistique implicite qui réside dans le choix répété d'une valeur donnée pour le coefficient de sécurité.

Lorsque l'on désire une fiabilité élevée et de hautes performances, ce procédé apparaît inadéquat car ne tenant pas compte de la dispersion des efforts et des résistances.

Les forces appliquées sont dispersées en raison des hypothèses de la "Résistance des Matériaux" (homogénéité et isotropie des matériaux) et de la dispersion des caractéristiques géométriques des structures.

D'autre part, la dispersion des caractéristiques des matériaux s'explique par la nature même de ces derniers. Leurs caractéristiques sont fonction des lacunes réparties aléatoirement en leur sein. On sait, en effet, que dans le cas des matériaux très purs et très homogènes, cas des trichites

(ou wiskers), on constate des résistances des dizaines de fois supérieures aux valeurs courantes.

- Fiabilité des systèmes mécaniques

.- Estimation de la fiabilité

Elle est justiciable des mêmes méthodes statistiques que celles utilisées en électronique.

.- Prédiction de la fiabilité

Si la fiabilité des composants est connue, les méthodes utilisées en électronique sont applicables, c'est-à-dire établissement d'un diagramme bloc de fiabilité auquel on applique le calcul des probabilités.

La notion de redondance utilisée en électronique se traduit par la notion de système fail-safe pour les structures mécaniques. Cela signifie par exemple qu'une poutre maîtresse sera remplacée par n poutres placées en parallèle de telle sorte que si l'une vient à se rompre, les efforts sont repris par les n - 1 poutres restantes avec toutefois un coefficient de sécurité moindre, il est vrai, mais suffisant pour achever la mission.

Le principe fail-safe est particulièrement utilisé en aéronautique.

Outre ce type de redondance, un moyen d'améliorer la fiabilité est de déterrer les organes, c'est-à-dire de les utiliser sous des charges inférieures à leur charge nominale.

Pour les systèmes informationnels, les méthodes d'analyse de variation des paramètres sont applicables dès que l'on dispose d'un modèle de fonctionnement. Ce modèle est généralement mathématique. Dans le cas d'un système hydraulique, par exemple, il s'agira des équations de la mécanique des

fluides. Lorsque les phénomènes sont en partie inconnus, il est possible de construire un modèle physique ou maquette à partir duquel on met au point une expression mathématique convenable pour la fonction de transfert.

La possession d'un modèle est extrêmement intéressant car il permet de déterminer l'évolution des performances du système en fonction de l'état des organes composants. Cette connaissance permet d'apparier les organes composants d'un dispositif neuf pour avoir les performances optimales ou de déterminer les cotes d'une pièce de rechange pour maintenir à l'optimum les performances d'un système qui n'est pas totalement rénové.

Ce genre de détermination nécessite généralement l'usage d'un ordinateur.

Amélioration de la fiabilité.-

L'analyse des sources de panne et de leurs conséquences pour un système, et la connaissance des sources de panne et de leurs conséquences pour des systèmes semblables permettent d'améliorer la fiabilité des systèmes mécaniques en améliorant les règles de l'art pour la construction et le choix des parties les plus vulnérables.

A titre d'exemple, on trouvera ci-dessous quelques renseignements de cette nature tirés de la référence A.2. pour deux types d'installation, c'est-à-dire la répartition des pourcentages des premiers organes défaillants.

Compresseur centrifuge d'installations d'air conditionné.-

- Paliers de butée	36 %
- Vanne d'admission	22 %
- Paliers portant des charges radiales	14 %
- Diffuseur	11 %
- Accouplement	8 %
.....	

Compresseur centrifuge (process).-

- Paliers	62,4 %
- Rouet	18,8 %
- Etanchéité sur l'arbre et accouplement	18,8 %

6 - SUGGESTIONS POUR UN PROGRAMME D'ETUDE

De ces quelques remarques, nous conclurons que, pour améliorer la fiabilité des ensembles mécaniques, il est souhaitable :

- d'établir des statistiques sur les causes et les conséquences des défaillances d'organes dans des installations existantes.

- d'obtenir une meilleure connaissance de la dispersion des caractéristiques des matériaux et cela grâce à des essais systématiques.

- d'étudier la loi de fiabilité des organes les plus courants.

- d'étudier les fonctions de transfert des systèmes les plus courants.

- d'entreprendre une étude bibliographique sur tous les sujets ci-dessus.

REFERENCES

A - Sur la fiabilité mécanique ou électromécanique

1. Statistical models in mechanical reliability
by John H.K. KAO
National Symposium on reliability and quality control

2. Loss prevention
Vol. 2
Prepared by Editors of Chemical Engineering Progress
A CEP technical manual published by American Institute of Chemical Engineers

3. Les gyroscopes mécaniques
Mémorial de l'Artillerie française, 4ème fasc 1964
Paris Imprimerie Nationale - 1964 -
Communication présentée au cours de la "Semaine d'études sur les gyroscopes mécaniques" organisée par le CNES du 20 au 23 Avril 1964

4. Fiabilité
par René METTHEY
(Fiabilité de lignes d'arbres et de batteries)
dans "l'Industrie des voies ferrées et des transports automobiles"
et dans "Arts et Métiers"
Avril 1968

5. Mechanical reliability concepts
ASME Conference
New York, 17/20 May 1965

6. Reliability prediction for mechanical and electromechanical parts
Technical documentary report n° RADC TDR 64-59 FR
George CHERNOWITZ

7. L'interprétation des essais d'endurance grâce aux techniques de fiabilité
par M. Michel VIGIER
Journal de la S.I.A. - 39ème année - tome XXXVIII - n° 2
Février 1965

8. Techniques de fiabilité et essais d'organes
par M. Sully SCHACHTER
Journal de la S.I.A. - 40ème année - tome XXXIX - n° 12
Décembre 1966

9. Influence de la fiabilite des systèmes sur les risques d'accidents dûs à un manque de qualités de vol
par M. J.C. WANNER
L'Aéronautique et l'Astronautique - 1968 - n° 7

10. La fiabilité en aéronautique et en astronautique
par M.A. MIHAIL
dans "l'Aéronautique et l'Astronautique" - 1968, 7 et 1969, 1 - 8

11. A reliability prediction method for propulsion systems
Reliability Engineering - p. 322-342
ARINC research corporation

12. Dimensionless parameter reliability analysis and application to mechanical creep
by R. SIMON
Journal of Basic Engineering - ASME - March 1966

13. Inference from the third failure in a sample of 30 from a Weibull distribution (Ball bearings endurance tests)
by John I. Mc COOL
Industrial Quality Control - Sept. 1966

14. Specifying reliability for shipboard electric rotating equipment
by Floyd D. ANDERSON
Bu Ships Journal - July 1965

15. Ship propulsion reliability and availability analysis
by R.L. HAMILTON
Annual Symposium on reliability - 1968

16. Effectiveness of ship systems and machinery
by I. BAZOVSKY and Glenn E. HENE
Annual Symposium on reliability - 1968

17. Availability assessment of nuclear plants
by W.R. LAHS and R.M. CHLETNKAMP
Annals of assurance sciences 1968
Seventh reliability and maintainability conference.
Published by ASME - San Francisco, California
July 14-17 1968

18. A reliability prediction method for propulsion system
Reliability engineering - ARINC Research Corporation, p. 322
Ed. by Prentice HALL

19. Proposed procedure for reliability stress analysis of mechanical and electro mechanical devices
I. KIRKPATRICK -
RCA - Victor Co Ltd, Dept n° 176
Feb. 27 (1958)

20. A practical approach to reliability in turbomachinery
James C. RIPLE (Garrett Corp. Air Research Manufacturing Div. Los Angeles, California)
Society of automotive engineers, National Aeronautic and space engineering and manufacturing
Meeting Los Angeles, Cal.
Sept. 23-27, Paper 744 D, 11 p (1963)

21. Reliability of a single degree of freedom mechanical system
W.H. BLEUEL Jr (Endevco Corp. Pasadena, Calif.)
Institute of Electrical and electronics engineers, International Conf. exhibit on aerospace support, Washington, D.C. Aug. 4-9, 1963
IEEE - Transactions on aerospace, vol. AS - 1, Aug. (1963)
p. 575-579

22. Reliability through statistical material property definition
H.G. POPP (General Electric Co, Large jet Engine Dp)
Society of automotive engineers, national aeronautics and space Engineering. Manufacturing meeting
Los Angeles. Calif. Oct. 8-12, paper 580 B, 9 p, 1962

23. Statistical investigation of the fatigue life of deep-grove ball bearings
J. LIEBLEIN and M. ZELEN
J. Res. Nat. Bur. Stand 57, n° 5, p. 275-316 (1956)

24. New concepts in the prediction of mechanical and structural reliability
Arnold A. ROTHSTEIN (AVCO Corp. WILMINGTON, Mass)
AIAA - SAE - ASME, Aerospace reliability and maintainability Conf. 1st, Washington DC, May 6-8 (1963)
New York, American Institute of aeronautics and astronautics, p. 91-97 - 11 ref. (1963)

25. Nuclear power plant reliability
HEFFLRSON G.
Nuclear engineering Apr. 1963

26. Estimates of error for design reliability
by Bruce L. BAIRD and William N. Mc LEOD
Proc. 20th National Symposium on reliability and quality Control (ASQC) Jan. 7-8-9 1964 Washington

B - Sur la fiabilité en général

1. Reliability handbook
Edited by Grant IRESON
Mac Graw Hill Company

2. Méthode pratique d'estimation statistique des lois de survie
par J.L. BELLON
Revue Française de recherche opérationnelle
9ème année - 2ème trimestre 1965 - n° 35

3. Systems reliability
by N.E. GOLOVIN
Industrial Quality Control - May 1964

4. A survey of techniques for analysis and prediction of equipment reliability
by ELMORE KLANTON and Richard M. JACOBS
Industrial Quality Control - Dec. 1962

5. Reliability Data processing and reporting in industry
By IRVIN R. WHITEMAN
Industrial Quality Control, Dec. 1964

6. La fiabilité des systèmes
par P. CHAPOUILLE et R. de PAZZIS
Ed. MASSON 1968